Exhibit 6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh et al.	Attorney Docket No.: 39843-0183IP1
U.S. Patent No.:	9,609,510	
Issue Date:	March 28, 2017	
Appl. Serial No.:	14/208,236	
Filing Date:	March 13, 2014	
Title:	AUTOMATED CREDENTIAL PORTING FOR MOBILE DEVICES	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 9,609,510 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

LIST OF EXHIBITS

EX1001	U.S. Patent No. 9,609,510 to Raleigh ("the '510 Patent")
EX1002	Excerpts from the Prosecution History of the '510 Patent ("the Prosecution History")
EX1003	Expert Declaration and Curriculum Vitae of Patrick Traynor, Ph.D.
EX1004	U.S. Publication No. 2009/0217364 ("Salmela")
EX1005	U.S. Publication No. 2013/0165075 ("Rishy-Maharaj")
EX1006	U.S. Publication No. 2010/0029273 ("Bennett")
EX1007	U.S. Publication No. 2012/0236760 ("Ionescu")
EX1008	U.S. Publication No. 2010/0222024 ("Sigmund")
EX1009	U.S. Publication No. 2010/0177663 ("Johansson")
EX1010	U.S. Patent No. 9,191,394 ("Novak")
EX1011	U.S. Publication No. 2009/0253409 ("Slavov")
EX1012	Federal Communications Commission (FCC) Regulation (2010), *available at*, https://www.govinfo.gov/content/pkg/FR-2010-06-22/pdf/2010-15073.pdf ("FCCReg")
EX1013	U.S. Publication No. 2011/0130119 ("Gupta")
EX1014	U.S. Publication No. 2008/0122796 ("Jobs")
EX1015	Samsung Galaxy SII Mobile Phone User Manual (2011), *available at* https://ringtones.specialtyansweringservice.net/wp-content/uploads/2014/08/manuals/samsung-galaxys2-userguide.pdf

EX1016	iPhone User Guide For iPhone OS 3.1 Software (2009), *available at* https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf
EX1017	Architecture and Enablers for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks (2009), *available at* https://www.researchgate.net/publication/224371987_Architecture_and_Enablers_for_Optimized_Radio_Resource_Usage_in_Heterogeneous_Wireless_Access_Networks_The_IEEE_19004_Working_Group
EX1018	Characterizing Radio Resource Allocation for 3G Networks (2010), *available at* https://www.cs.columbia.edu/~lierranli/coms6998-7Spring2014/papers/RRC3G_imc2010.pdf
EX1019	Operating System Implications of Fast, Cheap, Non-Volatile Memory (2011), *available at* https://www.usenix.org/legacy/events/hotos11/tech/final_files/Bailey.pdf
EX1020	iPod touch User Guide for iOS 5.1 Software (2012), *available at* https://cdsassets.apple.com/live/6GJYWVAV/user/ma1627_ipod_touch_ios5_user_guide.pdf
EX1021	Samsung Galaxy SIII 4G LTE Smartphone User Manual (2013), *available at* https://downloadcenter.samsung.com/content/UM/202101/20210101045744723/ATT_SGH-I747_Galaxy_SIII_English_User_Manual_KK_NE4_F1.pdf
EX1022	U.S. Publication No. 2009/0249247 (“Tseng”)
EX1023	U.S. Patent No. 7,280,818 (“Clayton”)
EX1024	U.S. Patent No. 8,923,824 (“Masterman”)

EX1025	RESERVED
EX1026	Samsung's Stipulation Regarding Invalidity Grounds in Co-Pending District Court Litigation
EX1027	Jacob et al., *Memory Systems: Cache, DRAM, Disk* (2007) ("Jacob")
EX1028	U.S. Publication No. 2012/0185636 ("Leon")
EX1029	U.S. Patent No. 8,060,748 ("Johansson-748")
EX1030	U.S. Publication No. 2006/0258289 ("Dua")
EX1031	European Telecommunications Standards Institute (ETSI) Technical Specification 23.003 v8.11.0 (2011), *available at* https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/08.11.00_60/ts_123003v081100p.pdf
EX1032	Control Servers in the Core Network (2000), *available at* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1247211968f9167dbc5e7ea896bd910762e57ba7
EX1033	Wireless Application Protocol (WAP) Architectural Overview (2001), *available at* https://www.openmobilealliance.org/release/Push/V2_1-20051122-C/WAP-250-PushArchOverview-20010703-a.pdf
EX1034-1099	RESERVED
EX1100	Complaint for Patent Infringement in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al*., 2-24-cv-00228 (EDTX) (Apr. 03, 2024)
EX1101	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings, June 21, 2022, *available at* https://www.uspto.gov/sites/default/files/documents/interim_pr

	oc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf
EX1102	Docket Control Order in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al*., Case No. 2:24-cv-00228 (EDTX) (Aug. 9, 2024)
EX1103	Disclosure of Asserted Claims and Infringement Contentions in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al*., 2-24-cv-00228 (EDTX) (Jul. 11, 2024)

LIST OF CHALLENGED CLAIM ELEMENTS

Claim 1	
[1pre]	A wireless device, comprising:
[1a]	a user interface;
[1b]	memory configured to store:
[1c]	one or more credentials associated with the wireless device, the one or more credentials for authorizing the wireless device to use a wireless access network to access one or more services, and
[1d]	a target credential; and
[1e]	one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to:
[1f]	obtain, through the user interface, an indication of a user request to replace a particular credential of the one or more credentials with the target credential,
[1g]	detect a network-provisioning state change, and based on the detected network-provisioning state change, automatically
[1h]	determine that the particular credential does not match the target credential,
[1i]	initiate a programming session with a network element communicatively coupled to the wireless device over the wireless access network,
[1j]	obtain an updated credential from the network element, and
[1k]	assist in storing, in memory, the updated credential as the particular credential.
Claim 2	

[2]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: determine that the updated credential does not match the target credential, and based on the determination that the updated credential does not match the target credential, take an action.
Claim 3	
[3]	The wireless device recited in claim 2, wherein the action is to communicate with the network element.
Claim 6	
[6]	The wireless device recited in claim 2, wherein the action is to at least assist in restricting communications by the wireless device over the wireless access network.
Claim 7	
[7]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: determine that the updated credential matches the target credential, and based on the determination that the updated credential matches the target credential, take an action.
Claim 11	
[11]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a registration attempt initiated by the wireless device has failed.
Claim 14	
[14]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to authenticate with the network element has failed.
Claim 15	

[15]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to be authorized for a service has failed.
Claim 16	
[16]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a network access error has occurred.
Claim 17	
[17]	The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises receiving a provisioning-state-change message.
Claim 18	
[18]	The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a text message.
Claim 19	
[19]	The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a push message from a push server communicatively coupled to the wireless device over the wireless access network.
Claim 20	
[20]	The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a message received by an application program on the wireless device.
Claim 21	
[21]	The wireless device recited in claim 1, wherein the one or more credentials comprise a phone number.
Claim 22	

[22]	The wireless device recited in claim 1, wherein the one or more credentials comprise an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.
Claim 23	
[23]	The wireless device recited in claim 1, wherein the target credential comprises a phone number.
Claim 24	
[24]	The wireless device recited in claim 1, wherein the target credential comprises an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.
Claim 25	
[25]	The wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number.

Claim 28	
[28]	The wireless device recited in claim 1, wherein the user interface comprises a display.
Claim 29	
[29]	The wireless device recited in claim 1, wherein the user interface comprises a speaker.
Claim 30	
[30]	The wireless device recited in claim 1, wherein the one or more services comprise a voice service, a messaging service, or a data service.
Claim 31	
[31]	The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an application program.
Claim 32	
[32]	The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an operating system (OS) component, an OS function, an OS service, a modem programming agent, a modem software or firmware agent, an over-the-air (OTA) mobile device parameter programming agent, an Open Mobile Alliance (OMA) agent, a secure communication agent configured to communicate number porting and number provisioning information, a software agent, a firmware agent, or a combination of these.
Claim 33	
[33]	The wireless device recited in claim 1, wherein the user request comprises an indication of the target credential, a phone number, a user name, a password, an account number, a subscriber name, a company name, at least a portion of a billing address, at least a portion of a social security number, a personal identification number (PIN), or a combination of these.
Claim 35	

[35]	The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information associated with the user request through the user interface**.**
Claim 36	
[36]	The wireless device recited in claim 1, wherein the network element comprises a programming server.
Claim 37	
[37]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using at least a portion of the one or more credentials associated with the wireless device.
Claim 38	
[38]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a temporary credential.
Claim 39	
[39]	The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from memory.
Claim 41	
[41]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a default credential.

Claim 42	
[42]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over the wireless access network.
Claim 43	
[43]	The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over a Wi-Fi network.
Claim 45	
[45]	The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to at least assist in restricting communications over the wireless access network until the updated credential has been obtained.
Claim 46	
[46]	The wireless device recited in claim 1, wherein the target credential comprises a configuration state indicator.
Claim 47	
[47pre]	A non-transitory computer-readable storage medium storing one or more machine-executable instructions that, when executed by one or more processors of a wireless device, cause the one or more processors to:
[47a]	obtain, through a user interface, an indication of a user request to replace a particular credential of one or more credentials, for authorizing the wireless device to use a wireless access network to access one or more services, with a target credential;

[47b]	detect a network-provisioning state change; and based on the detected network-provisioning state change, automatically
[47c]	determine that the particular credential does not match the target credential,
[47d]	initiate a programming session with a network element communicatively coupled to the wireless device over a wireless access network,
[47e]	obtain an updated credential from the network element, and
[47f]	assist in storing, in memory, the updated credential as the particular credential.
Claim 48	
[48]	The wireless device of claim 1, wherein the memory configured to store the one or more credentials comprises a protected memory that does not allow direct user modification of the particular credential.

Samsung Electronics Co., Ltd. ("Petitioner" or "Samsung") petitions for *Inter Partes* Review ("IPR") of claims 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48 ("the Challenged Claims") of U.S. Patent No. 9,609,510 ("the '510 Patent").

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the '510 Patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR.

B. Challenge and Relief Requested

Petitioner requests IPR on Ground 1A listed below:

Ground	Claims	Basis
1A	1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, 45-48	§103 – Obvious based on Salmela (EX1004) in view of Rishy-Maharaj (EX1005)

Ground 1A is further supported by the expert declaration of Patrick Traynor, Ph.D. (EX1003), and the additional evidence cited herein.

The '510 Patent was filed on March 13, 2014, claiming priority to a provisional application filed on March 14, 2013. Without conceding that the '510 Patent is entitled to the benefit of the provisional application's filing date, Petitioner nonetheless treats March 14, 2013 as the Critical Date of the Challenged Claims for purposes of the analysis in this Petition. Ground 1A relies on

publications that all qualify as prior art under pre-AIA 35 U.S.C. §102 as shown below:

Reference	Filed	Published	Pre-AIA Prior Art Status
Salmela	06/17/2008	08/27/2009	§102(a)-(b), (e)
Rishy-Maharaj	05/23/2012	06/27/2013	§102(e)

II. SUMMARY OF THE '510 PATENT

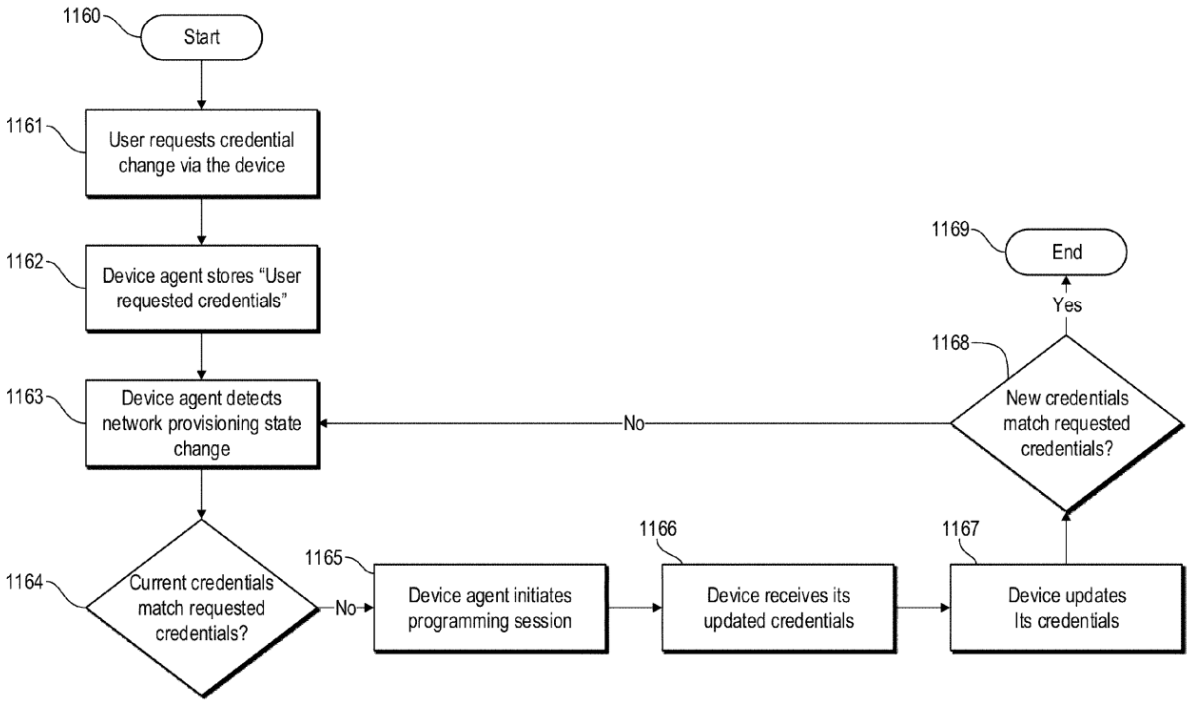
A. Brief Description

The '510 Patent describes techniques for automatically updating network access credentials for a wireless device (e.g., a mobile phone). EX1001, 5:10-6:57, 6:4-7:15, 9:4-10:56, 11:20-12:44; EX1003, ¶24. The credentials can include, for example, an international mobile subscriber identity (IMSI), a phone number, or an internet protocol (IP) address. EX1001, 5:21-48, 9:59-10:8.

In some embodiments, the user submits a request to update the credentials on a wireless device through a user interface of the device itself. EX1001, 7:28-68, 10:57-67, FIG. 3; EX1003, ¶25. The device can continue to operate on its current (non-updated) credentials for a time while the user's request is processed by a service provider. EX1001, 9:4-35, 10:57-11:27. Eventually, however, the current credentials will expire or be deactivated by the service provider pursuant to the user's request, and consequently, the device will be unable to gain access to the network using its current credentials. EX1001, 9:4-35, 10:57-11:27. The device

can interpret such a failure to access the network with its current credentials as a "network provisioning state change," and in response, the device automatically initiates operations to update its credentials as shown in FIG. 3:

FIG. 3



EX1001, FIG. 3.

As depicted above, the wireless device can perform several actions upon detecting a network provisioning state change. EX1001, 11:38-12:33. These actions can include determining whether the device's current credentials match the user-requested credentials, initiating a programming session with a network element, receiving updated credentials, and determining whether the updated credentials match the user-requested credentials. EX1001, 11:38-12:33. The '510

Patent explains that credentials can be updated "automatically" and "without informing the subscriber" in some embodiments. EX1001, 12:34-35. Consequently, apart from the initial step of receiving a user request to update credentials, the wireless device can automatically perform the subsequent operations depicted in FIG. 3 to update the device's credentials without user participation. EX1001, 10:57-12:44; EX1003, ¶26.

B. Prosecution History

The Examiner issued just one office action during original examination of the '510 Patent. EX1002, 445-458, 497-504; EX1010; EX1003, ¶27-31. The applicant responded with amendments clarifying that (i) the "determine," "initiate," "obtain," and "assist" steps recited in the independent claims are performed "automatically" in response to detecting the network-provisioning state change, and (ii) the one or more credentials are for "authorizing" the wireless device to "use a wireless access network to access one or more services." EX1002, 450, 457. Although the Examiner issued a notice allowing the application following the applicant's response, the application never should have been allowed. This Petition compellingly demonstrates that the prior art renders each of the Challenged Claims obvious. EX1003, ¶31.

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art ("POSITA") for the '510 Patent by the Critical Date (March 14, 2013) would have had a Bachelor's degree in electrical engineering, computer engineering, computer science, or equivalent, and two years of industry experience in networking security, mobile device communications security, and/or wireless digital communications systems security. EX1003, ¶21. Additional education might compensate for less experience, and vice versa. EX1003, ¶21-22.

IV. CLAIM CONSTRUCTION

Petitioner acknowledges that claim terms in an IPR are construed consistent with the *Phillips* standard applied in district court proceedings. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. Considering the substantial overlap between the preferred embodiments of the '510 Patent and the prior art combinations advanced in Ground 1A of this Petition, Petitioner submits that no claim terms presently require formal constructions for purposes of resolving controversies in this proceeding. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Google Inc. v. Intellectual Ventures II LLC*, 701 Fed. Appx. 946, 956 (Fed. Cir. 2017) ("do not require construction" to "resolv[e] the parties' patentability arguments"); EX1003, ¶23.

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each Challenged Claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning indefiniteness or claim scope that can only be raised in district court or otherwise outside the context of an IPR. *Mylan Pharm. Inc. v. Horizon Pharma USA, Inc*., IPR2018-00272, Paper 35, 6-8 (PTAB 2019). The Board has regularly compared indefinite claims to the prior art for purposes of considering unpatentability. *See, e.g.*, *Chicago Mercantile Exchange, Inc. v. 5th Market, Inc*., CBM2013-00027, Paper 33, 3 (PTAB 2014); *SAP America, Inc. v. Lakshmi Arunachalam*, CBM2013-00013, Paper 61, 29 (PTAB 2014). For this petition, Petitioner applies prior art in a manner consistent with Patent Owner's allegations of infringement before the district court.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A: Salmela in view of Rishy-Maharaj would have rendered obvious claims 1-3, 6-7, 11, 14-25, 28-33, 35-39, 41-43, and 45-48

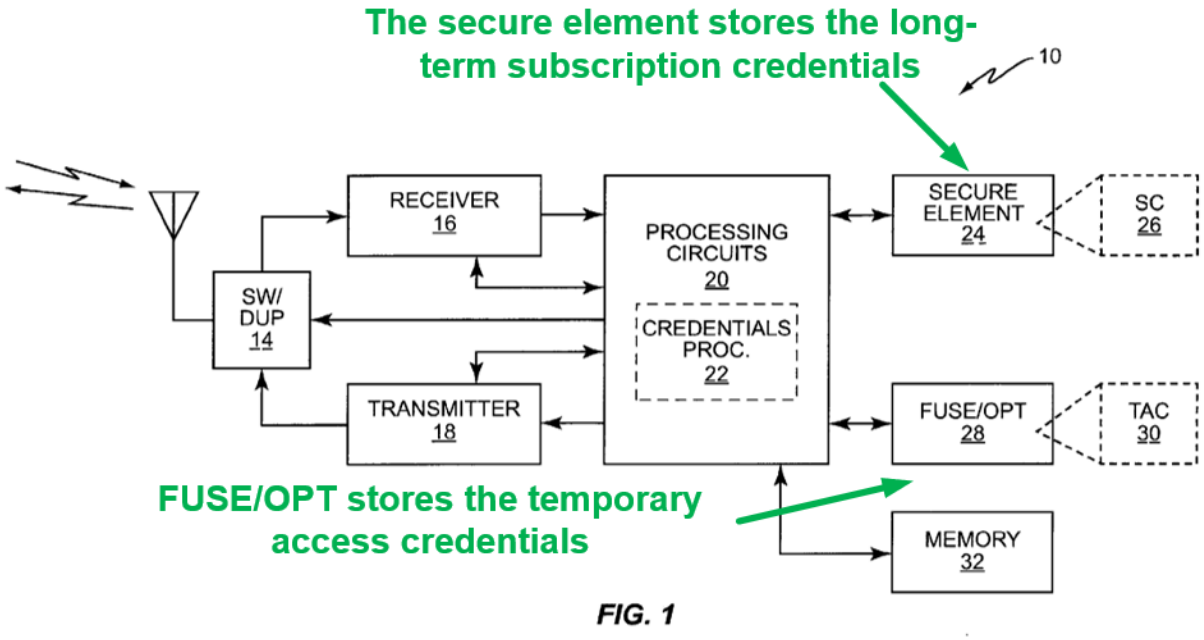
1. *Salmela*

Like the '510 Patent, Salmela describes techniques for automatically updating credentials on a wireless device. EX1004, [0003]-[0012], [0020]-[0027]; EX1003, ¶32-36. According to Salmela, "[s]ecure and convenient management of subscription credentials [stood] as an ongoing challenge in the field of wireless communications." EX1004, [0003]. Salmela also explains that "subscription

credentials … link the device to a given network service provider (home operator) and allow it to authenticate itself to the operator's home network, and to any number of visited networks, subject to roaming agreements, etc." EX1004, [0003]. Recognizing that it is sometimes difficult for device owners to manually update subscription credentials when they "chang[e] subscription plans, and particularly when changing home operator affiliations," Salmela proposes a credential updating process that is automatically triggered upon detecting "a failure to gain network access." EX1004, [0009]; [0027], *generally* [0020]-[0027], FIG. 2.

In Salmela's process, the wireless device is configured to "revert[] from subscription credentials to temporary access credentials, in response to detecting an access failure." EX1004, [0010]; EX1003, ¶34. Such network access failure can occur when the device's current subscription credentials expire or are otherwise no longer valid to authenticate the device on the network under the subscription plan that the device had been operating on previously, which can result from the device owner having changed subscription plans to a new home operator. EX1004, [0010]; EX1003, ¶35. "The device [then] uses [] temporary access credentials to gain temporary network access," and if "the device determines [that] it needs new subscription credentials," it "uses the temporary access to obtain them." EX1004, [0010], *see also*, [0011]-[0013], [0020]-[0028], [0031], FIGS. 1-2, 4. For example, temporary network access allows the device to (1) determine that new subscription

credentials are needed, (2) initiate a programming session with a credentialing server if it is determined that new subscription credentials are needed, (3) obtain the new subscription credentials from the credentialing server, and (4) download the new subscription credentials to a secure element in a memory of the device. EX1004, [0024], [0025], [0041].



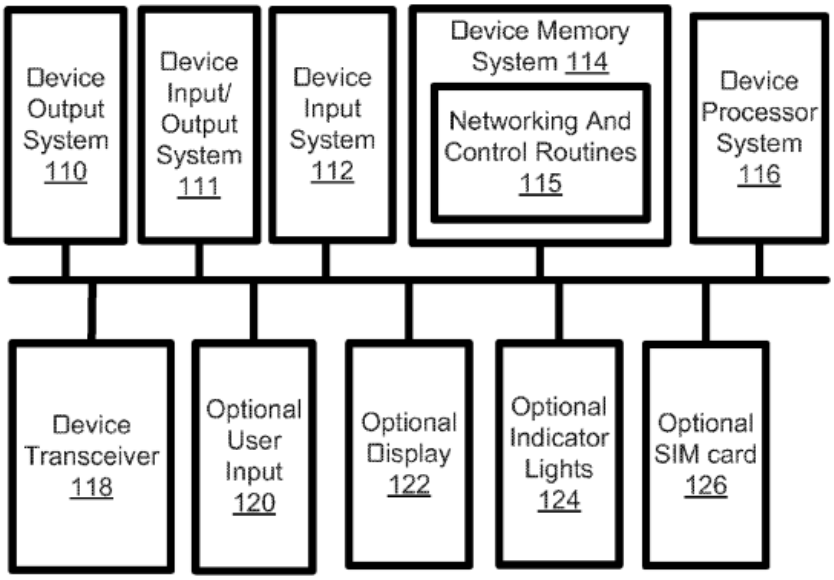
EX1004, FIG. 1.

With this process, Salmela allows "a device owner" to "change subscriptions without having to first update the affected device." EX1004, [0050]. In particular, when the device owner changes subscriptions, each device associated with the changed subscription automatically updates its own credentials by performing Salmela's process of detecting network access failure, reverting to temporary credentials, and updating to new credentials associated with the changed

subscription. EX1004, [0011] ("To the extent that any subscription agreement change invalidates device-held subscription credentials, each such device will detect access failure with its current subscription credentials and revert to temporary access credentials and contact a registration service or other entity to determine if new subscription credentials are needed."), [0024], [0025], [0041]; EX1003, ¶36.

2. *Rishy-Maharaj*

As with Salmela and the '510 Patent, Rishy-Maharaj describes techniques for updating credentials on a wireless device according to a user-selected subscription plan. EX1004, [0010]-[0012]; EX1005, [0028]-[0036]; EX1003, ¶37. Although Salmela does not describe in detail how the user initiates a request to change subscription plans or the home operator, Rishy-Maharaj explains that the request can be submitted through a user interface of a wireless device. EX1005, [0108]-[0121]. For example, Rishy-Maharaj describes a user interface of a wireless device that "list[s] services…for the user to select" and that allows "the user to select a plan." EX1005, [0112]; *see also*, ("[T]he user may select the subscription plan and network that best suits the user."). The user interface of the device may include a "device output system," a "device input system," an "optional user input," and an "optional display," like that depicted below in FIG. 1B:



EX1005, FIG. 1B.

EX1005, [0058]-[0060], [0066], [0067], FIG. 1B.

3. *The Salmela-Rishy-Maharaj Combination*

As discussed above, Salmela discloses that the owner of one or more wireless devices can request to update a subscription plan used by those devices to access the wireless network(s) of an affiliated home operator. EX1004, [0008] ("the device owner can select and activate subscriptions"), [0009] ("changing subscription plans"), [0011] ("an owner … can change subscription agreements"), [0053] ("changing subscription information"), Abstract ("new home operator"); *supra*, §V.A.1. While Salmela does not expressly describe how the device owner submits a request to update the subscription plan, Rishy-Maharaj demonstrates that one known option was to input the request through a user interface of an affected wireless device. EX1005, [0111]-[0112]; *supra*, §V.A.2; EX1003, ¶38. It would

have been obvious to apply Rishy-Maharaj's teachings in this regard to Salmela such that Salmela's device owner would select to activate or change subscriptions through a user interface of a wireless device, thereby prompting each of the user's devices associated with the selected subscription plan to automatically obtain new subscription credentials as needed upon detecting a failure to gain network access with their current subscription credentials, according to the processes disclosed in Salmela. EX1003, ¶38. A POSITA would have combined the teachings of Salmela and Rishy-Maharaj in this manner for multiple reasons.

First, a POSITA would have recognized that implementing Salmela's wireless device to include a "user interface" (e.g., user input 120) as suggested by Rishy-Maharaj would be advantageous in allowing a user to activate or change subscription plans on the wireless device itself without requiring the user to interact with other devices or with a call center. EX1005, [0058]-[0060], [0066], [0067], FIG. 1B; EX1003, ¶39. This would make the process of activating or changing subscriptions more convenient to the user by reducing the time, burden, and resources that would otherwise be necessary for the user to activate or change subscriptions. EX1005, [0066]; EX1003, ¶39.

Second, implementing Salmela's wireless device to include a "user interface" (e.g., display 122) as suggested by Rishy-Maharaj would allow the wireless device to provide information to the user in a manner that would

conveniently guide the user's selection of a subscription plan. EX1005, [0067]; EX1003, ¶40. For example, the wireless device in the Salmela-Rishy-Maharaj combination can be advantageously "used for displaying information to the user about how to operate wireless device 102, about available local networks, prompts for proceeding through the process of selecting a local network, and/or adding funds to an established subscription." EX1005, [0067]; EX1003, ¶40. This information displayed by the wireless device would aid the user in selecting a subscription plan on a single device. EX1003, ¶40.

Third, implementing Salmela's wireless device to include a "user interface" (e.g., display 122) as suggested by Rishy-Maharaj would have been obvious as a predictable application of a known technique (e.g., enabling selection of a subscription plan through a user interface of a wireless device) to a known system as taught by Salmela to achieve merely predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (an alleged invention that "simply arranges old elements with each performing the same function it had been known to perform" is obvious); EX1003, ¶41.

Fourth, it would have been obvious for a POSITA to implement Salmela's wireless device with a user interface as suggested by Rishy-Maharaj because doing so represents one of a finite number of predictable solutions for receiving a user selection from a user. *KSR* at 417 ("When there is a design need or market pressure

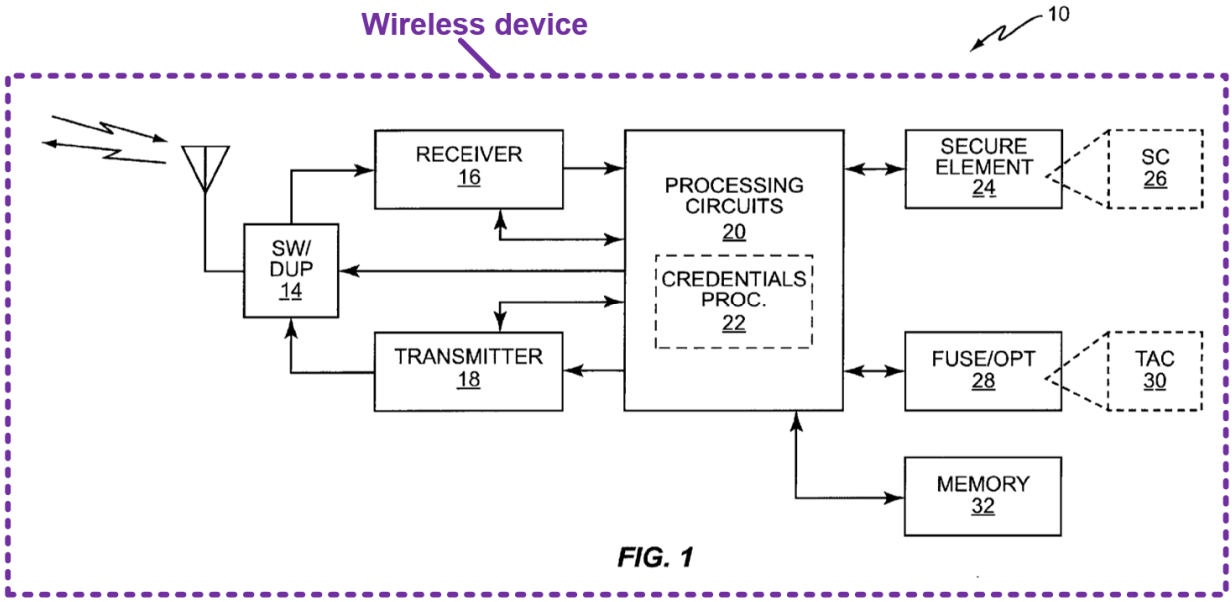
to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp." EX1003, ¶42. A POSITA would have appreciated, for example, that a request to change subscription plans for a wireless device could be made through a user interface of the wireless device itself, using another device, or by relaying the request to a third-party (e.g., a call center, retail outlet, or other agent of a network service provider). A POSITA would have been driven toward the first option in many cases for the reasons discussed above, including to promote user convenience in a straightforward manner. EX1003, ¶42.

A POSITA would have reasonably expected success implementing the Salmela-Rishy-Maharaj combination since wireless devices having user interfaces having hardware capable of executing software and performing the functions described above were well known before the Critical Date of the '510 Patent. EX1003, ¶43; *see also* EX1004, [0021], [0030].

4. *Application to Challenged Claims*

Element [1pre]

To the extent the preamble is a limitation, the Salmela-Rishy-Maharaj combination renders obvious the claimed "wireless device." EX1003, ¶95. For example, Salmela discloses a ***wireless*** communication ***device*** 10. EX1004, [0002], [0010], [0020]-[0025], [0027]-[0029], [0033]-[0047]; FIG. 1.



EX1004, FIG. 1 (annotated).

Element [1a]

To start, Salmela discloses that device 10 can be "a cellular communication device, such as a cellular radiotelephone, pager, PDA, computer." EX1004, [0021]. A POSITA would have recognized that these types of wireless devices all commonly included a ***user interface*** by 2013. EX1003, ¶96 (citing corroborating EX1014, EX1015, 10-15, EX1016, 28-31). Furthermore, Salmela acknowledges that a cellular handset user can "access subscribed services" through a home operator network. EX1004, [0004]. By 2013, accessing such "subscribed services" commonly involved interaction with a ***user interface*** on the wireless device (e.g., voice calls through a speaker and microphone, text messaging through a keypad and/or touchscreen, and internet browsing through a touchscreen). EX1003, ¶96

(citing corroborating EX1014, [0228]-[0300], [0544]-[0575], EX1015, 30, EX1016, 23).

To the extent Salmela does not expressly disclose that its wireless device includes a user interface, it would have been obvious to implement a user interface in Salmela's device based on the teachings of Rishy-Maharaj. EX1003, ¶97-99; *supra*, §V.A.3. Rishy-Maharaj, for example, describes a wireless device 102 that receives user inputs through a user interface of the device 102, e.g., user inputs for selecting subscription plans and managing credentials. *See, e.g.*, EX1005, [0028]-[0046], [0108]-[0121], FIGS. 1A, 1B, 2. Wireless device 102 includes several user interface elements including "device output system 110" and "device input system 112." EX1005, [0058]. Device output system 110 includes "a display system, a speaker system…and the like." EX1005, [0059]. Device input system 112 includes "a keyboard system…a mouse system, a track ball system…and the like." EX1005, [0060]. Other user interface elements of wireless device 102 include "optional user input 120" and "optional display 122." EX1005, [0058], [0066], [0067]. Aspects of the ***user interface*** of Rishy-Maharaj's wireless device 102 are depicted below in FIG. 1, for example:

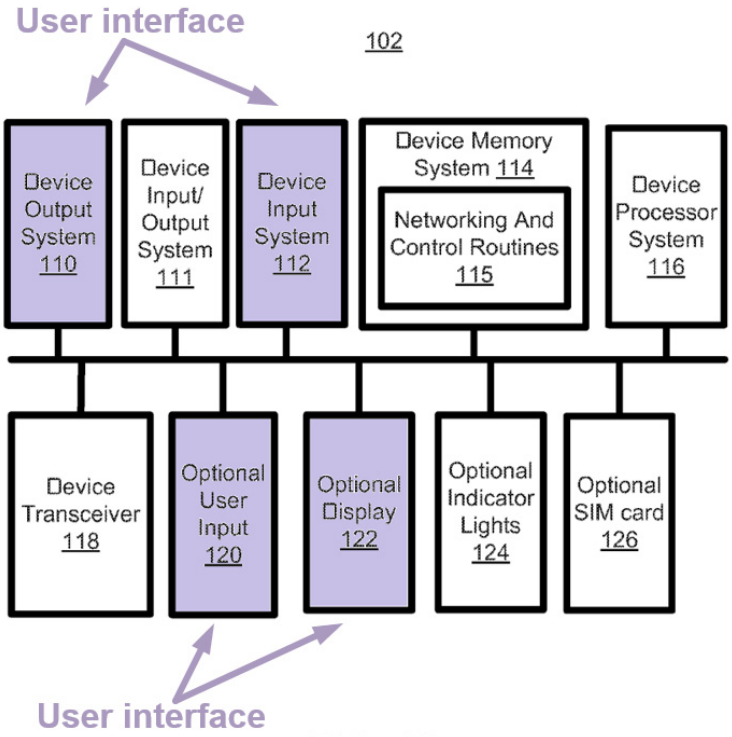


FIG. 1B

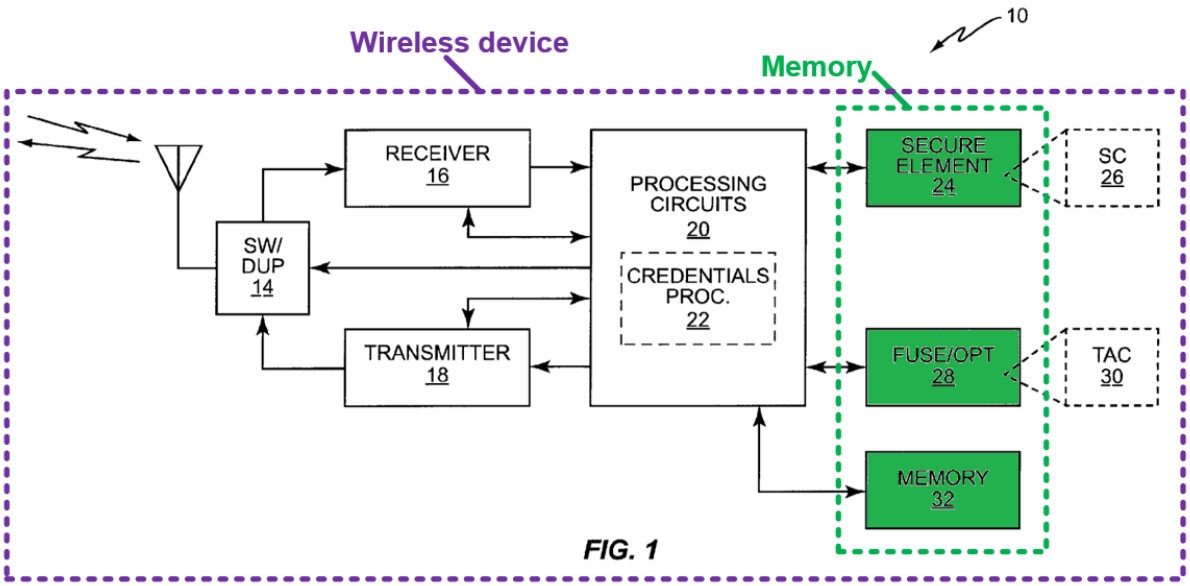
EX1005, FIG. 1B (annotated).

For at least the reasons discussed above (*see* §V.A.3), it would have been obvious and a POSITA would have been motivated to implement Salmela's device 10 to include a user interface as taught in Rishy-Maharaj. EX1003, ¶100. In the Salmela-Rishy-Maharaj combination, a user would beneficially be permitted to perform tasks such as activating or changing a subscription plan through the user interface of the wireless device. EX1003, ¶100.

Element [1b]

Salmela's device 10 has a ***memory*** that includes a secure element 24, a fuse/one-time-programmable (OTP) memory element 28, and a memory 32. EX1004, [0020], [0023], [0025], FIG. 1; EX1003, ¶101-102. According to

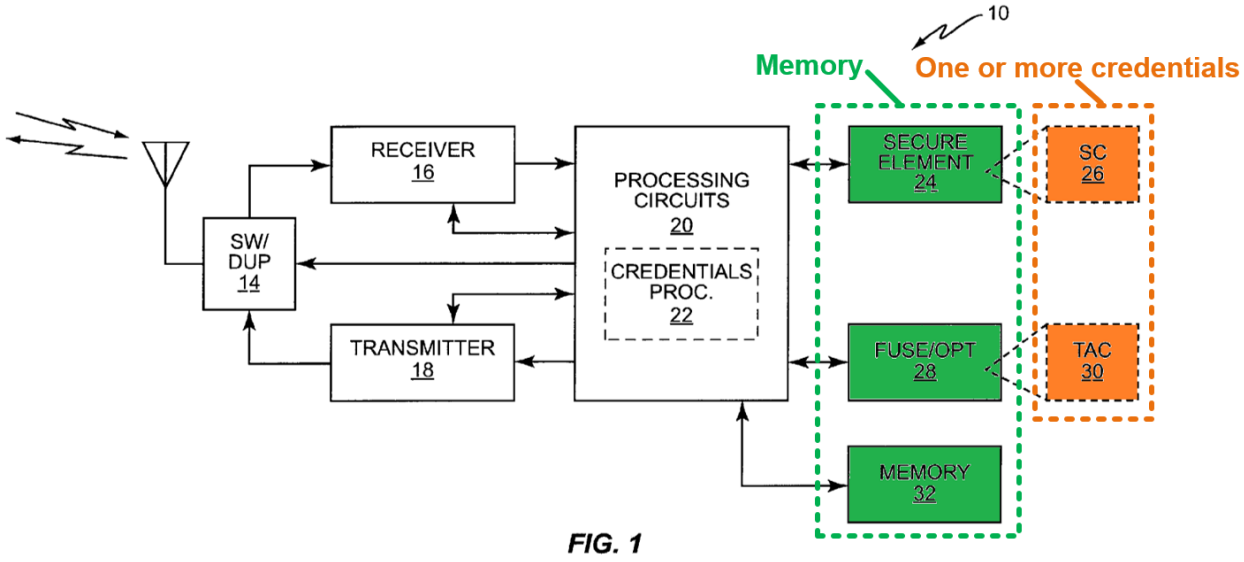
Salmela, secure element 24 can "***store*** subscription credentials (SC) 26," fuse/OTP memory element 28 can "***store*** temporary access credentials (TAC) 30," and memory 32 can "include one or more memory devices, for storing working data, computer program instructions, and configuration information." EX1004, [0020]. Numerous references corroborate that it was well-known in 2013 for wireless devices to have memory for storing information both persistently and temporarily, including registers, caches, random access memory, secure elements, and the like. EX1003, ¶102 (citing corroborating EX1014, [0095]-[0098], EX1015, 11, 12, 43, 44, EX1016, 146). Aspects of memory of Salmela's device 10 are depicted in FIG. 1, reproduced below. *Cf.* EX1001, 10:14-10:56 & FIG. 2 (explaining that the memory may provide for partitioned or integrated storage of subscription and interim credentials).



EX1004, FIG. 1 (annotated).

Element [1c]

The ***memory*** of Salmela's ***wireless device*** (e.g., device 10) is configured to store ***one or more credentials associated*** with device 10. EX1004, [0010]-[0012], [0020], [0022]-[0025], FIG. 1; EX1003, ¶103-106. For example, secure element 24 stores subscription credentials 26 and fuse/OTP memory element 28 stores temporary access credentials 30. EX1004, [0020], [0022]-[0025], [0027], FIG. 1. These credentials are depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

Salmela further explains that subscription credentials 26 and temporary access credentials 30 ***authorize*** Salmela's wireless communication device 10 to use a ***wireless access network*** to access ***one or more services***. EX1004, [0010]-[0012], [0020], [0022]-[0025]; EX1003, ¶104. For instance, Salmela expressly discloses that subscription credentials 26 are "for gaining network access" and that

temporary access credentials 30 are "for gaining temporary access." EX1004, [0022], *see also* [0012] ("the temporary access credentials are 'generic' credentials that allow temporary, limited network access"), [0025] ("uses those temporary access credentials 30 to gain temporary network access"). The "network access" described by Salmela provides device 10 access to a ***wireless access network*** such as a home network and/or a visited network. EX1004, [0010], [0028], [0030]-[0032].

For example, Salmela's device 10 can use subscription credentials 26 and temporary access credentials 30 to access home network 40 and visited network 46. EX1004, [0028], [0030]-[0032], FIG. 3. Home network 40 includes a radio access network (RAN) 42 and a core network (CN) 44. EX1004, [0028], FIG. 3. Visited network 46 includes RAN 48 and CN 50. EX1004, [0028], FIG. 3. These ***wireless access networks*** provide ***one or more services*** to device 10, such as wireless data service. EX1004, [0004], [0028], [0031]-[0033]; EX1003, ¶105-106. Access to the home and visited networks allows device 10 to connect to the internet and access the services of other networks and servers communicably coupled to the home and visited networks. EX1004, [0028] ("provide communicative coupling to one or more additional networks 52, such as the Internet"). Temporary access credentials 30 also authorize the device 10 to gain access to a wireless access network to utilize services for obtaining new long-term

subscription credentials 26. EX1004, [0028] ("for the purpose of acquiring new subscription credentials").

Element [1d]

As described above (*see* §V.A.1), Salmela discloses techniques for automatically updating subscription credentials 26 on a device 10. EX1004, [0003]-[0012], [0020]-[0027]; EX1003, ¶107. Device 10 can determine that new subscription credentials are needed by comparing "first information" corresponding to the subscription credentials 26 currently held by device 10 with "second information" corresponding to subscription credentials "that are considered by [a] registration service to be current for the wireless communication device 10." EX1004, [0044]; *see also*, [0041]. The first and second information may differ if the user has previously requested to change to a subscription plan requiring new subscription credentials that have not yet been loaded on device 10. EX1004, [0041], [0044].

According to Salmela, the "first information" can be a "hash value" or "time stamp" of the subscription credentials 26 currently held by device 10. EX1004, [0041], [0044]. Likewise, the "second information" can be a "hash value" or "time stamp" of subscription credentials that the registration service considers current for device 10. EX1004, [0041], [0044]. The hash value and/or time stamp of the underlying subscription credential that the registration service considers current

each corresponds to and renders obvious a "***target credential***" as recited in Element [1d]. EX1003, ¶108.

To this point, Salmela's hash value and/or time stamp for the subscription credentials considered current by the registration service are analogous and substantially similar to examples of the "requested credential" (e.g., target credential) as described in the '510 Patent specification.[1] EX1003, ¶109. For example, the '510 Patent explains that the wireless device can receive a requested credential from an "application server or other network element" and that the requested credential may contain only "a subset of information about all of the one or more credentials that were requested to be changed." EX1001, 11:1-19. Salmela's hash value and/or time stamp are likewise received from a remote server

[1] The term "target credential" is never used in the specification of the '510 Patent, but the descriptions of the "requested credential" in the specification generally align with the "target credential" in claim 1. FIG. 3, for instance, depicts an operation 1164 that involves comparing the device's current credentials with the requested credentials. EX1001, 11:28-37, FIG. 3. Element [1h] similarly refers to "determin[ing] that the particular credential does not match the target credential." EX1001, 20:33-34. Similar uses of "requested credential" and "target credential" occur throughout FIG. 3 and claim 1, respectively. EX1003, ¶109.

and contain a subset of information about the subscription credentials considered by the registration service to be current for device 10 to which the device owner has requested to change. EX1003, ¶109. The '510 Patent's disclosure at col. 11:32-37 is similarly clear that the requested credential (e.g., target credential) can be related but distinct from the underlying updated credential (e.g., IMSI) that the device uses to authorize itself on a wireless network. *See* EX1001, 11:32-37 (describing the "requested credential" as a "configuration state indicator" related to a phone number, ISDN, or other credential being updated).

Although claim 1 does not require that the "target credential" and underlying "updated credential" be the same, or even that the "target credential" and "updated credential" be similarly formatted, these features nonetheless would have been obvious in the Salmela-Rishy-Maharaj combination by implementing device 10 to receive the underlying subscription credentials (e.g., IMSI) that the registration service considers current for device 10, thereby allowing for direct comparison at device 10 between those credentials and the subscription credentials 26 currently held by the device (e.g., a direct IMSI comparison), rather than comparing time

stamps or hash values.[2] EX1003, ¶110. In this case, the underlying subscription credentials that the registration service considers current for device 10 would correspond to and render obvious the claimed "***target credential***." EX1003, ¶110.

In at least some cases, a POSITA would have been prompted to configure device 10 to receive and store the underlying credentials that the registration service considers current for device 10 in their original form in lieu of or in addition to a time stamp and/or hash value to facilitate a straightforward comparison of the credentials in their original form. EX1003, ¶111. This implementation would be beneficial to alleviate the burden on the remote server (e.g., registration server 54) of computing a hash or maintaining a time stamp for the credentials, thereby simplifying aspects of the registration service's operations. EX1003, ¶111. A POSITA also would have considered the choice of performing either a direct comparison of the credentials in their original form or a comparison of values associated with or derived from the credentials (e.g., hash values, time stamps) to be an obvious design choice for which a suitable option would be selected based on the needs and circumstances of a given application or design.

[2] As another predictable option, it would have been obvious for device 10 to compute hash values of both sets of credentials locally for comparison. EX1003, ¶110.

EX1003, ¶112. Comparing subscription credentials in their original form or comparing related values such as hashes or time stamps that uniquely represent the underlying subscription credentials would have been understood to equivalently indicate whether device 10 needs to update its current subscription credentials 26. EX1004, [0041], [0044]; EX1003, ¶112. Both options also would have been obvious to a POSITA, especially since Salmela itself already contemplates a range of options for comparing the device's current credentials to a target credential to determine whether new subscription credentials are needed on the device. EX1004, [0043] ("***Broadly***, the wireless communication device 10 … is configured to communicate with the registration service to determine whether new subscription credentials are needed."); *generally*, [0040]-[0045]; EX1003, ¶112.

Salmela also discloses that device 10 receives from the registration server 54 the hash value or time stamp for the credentials that the registration service considers current before comparing that information to the hash value or time stamp of the subscription credentials 26 currently held by device 10. EX1004, [0040], [0041]. A POSITA would have understood this to mean that the memory of device 10 stores the "second information" hash value or time stamp (e.g., target credential) at least temporarily upon receipt as the device 10 prepares to perform the comparison between the "first information" and "second information." EX1004, [0040]-[0041], [0044] ("second information received from the

registration service"); EX1003, ¶113. At the very least, it would have been obvious to store the second information or underlying subscription credentials that the registration service considers current in memory of device 10 for a period of time sufficient for device 10 to perform this comparison. EX1003, ¶113 (citing corroborating EX1027, 40). For example, it would have been obvious for device 10 to store the credentials or "second information" received from the registration server in registers, cache, random access memory, and/or or other memory of device 10 that conventionally make data available to a processor, as would occur for the device to 10 to perform the comparison described at paragraphs [0041] and [0044] of Salmela. EX1004, [0041], [0044], [0020] (memory 32 can "include one or more memory devices, for storing working data, computer program instructions, and configuration information"); *supra*, Element [1b]; EX1003, ¶114.

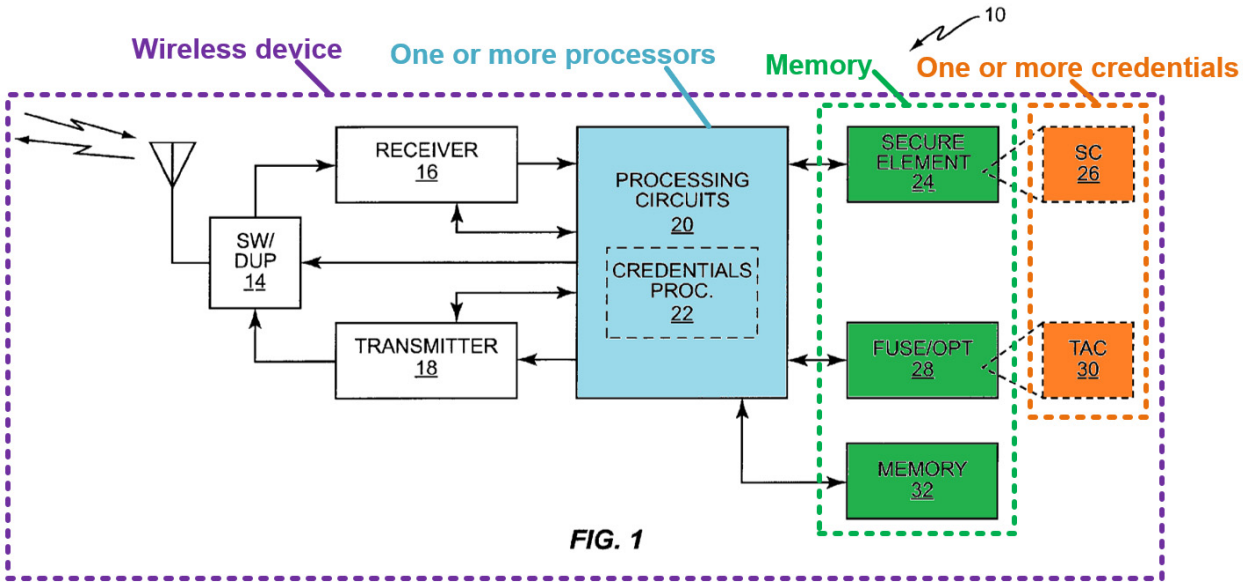
As another example, it would have been obvious to store the target credential (e.g., hash value, time stamp, or underlying credential) received from the registration service in secure element 24 or a similar memory element to keep such information secure and to ensure it is available for subsequent use, similar to the storage of subscription credentials 26 in secure element 24 as disclosed in Salmela. EX1004, [0020]; EX1003, ¶114.

Additionally, as described further below with respect to Element [1k], Salmela discloses and renders obvious storing the target credential that the

registration service considers current in the secure memory element 24 as an updated credential when device 10 determines that its current subscription credentials 26 are no longer valid. *Infra*, Element [1k]; EX1003, ¶115.

Element [1e]

Salmela's device 10 comprises ***one or more processors*** including processing circuits 20 and credentials processor 22. EX1004, [0020], [0024], [0026], [0027], FIG. 1; EX1003, ¶116-117. These ***one or more processors*** are depicted below in FIG. 1:



EX1004, FIG. 1 (annotated).

Salmela discloses that the ***one or more processors***–e.g., processing circuits 20 and/or credentials processor 22–***execute one or more machine-executable instructions*** that cause the ***one or more processors*** to perform actions. EX1004, [0020], [0024], [0026], [0027], FIG. 2. For instance, "credentials processor 22 may

be implemented via software executing in one or more microprocessor circuits used to implement the processing circuits 20." EX1004, [0026]. This software represents ***machine-executable instructions***. EX1003, ¶117. Furthermore, credentials processor 22 is configured to ***execute machine-executable instructions***. *See, e.g.*, EX1004, [0024] ("revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure"), [0034] ("controls or otherwise causes the device 10 to attempt a limited number of reattachments using its preferred network, and, if that fails, to attempt one or more additional reattachments to one or more non preferred networks"); EX1003, ¶117.

Element [1f]

Salmela describes that a user (referred to as "device owner") can request to activate or change subscription plans for each of his or her wireless devices. EX1004, [0008] ("the device owner can select and activate subscriptions"), [0009] ("changing subscription plans"), [0011] ("an owner … can change subscription agreements"), [0053] ("changing subscription information"), Abstract ("new home operator"), [0050] ("device owner can change subscriptions"), [0007]. After the user has submitted a request to change subscriptions, each device associated with the new subscription plan automatically obtains updated subscription credentials associated with the new subscription plan in response to detecting a network-

provisioning state change. EX1004, [0003]-[0009], [0011], [0020]-[0027], [0050], FIG. 3; EX1003, ¶118.

The user request to change a subscription plan to a new home operator in Salmela corresponds to and renders obvious "a user request to replace a particular credential of the one or more credentials with the target credential," as recited in [1f]. EX1003, ¶119. By requesting that the device 10 operate under a new subscription plan, the user is requesting that a subscription credential 26 currently held by device 10 (***a particular credential of the one or more credentials***) be replaced with a ***target credential*** associated with the new subscription plan, and indeed this would have been obvious to a POSITA since the new subscription plan is associated with a new home operator and thus requires new subscription credentials for the device to use a wireless access network to access services offered by the new home operator under the new subscription plan.[3] EX1004,

[3] As discussed in the analysis of [1d], Salmela's hash value or time stamp for the subscription credential that the registration service considers current, and the underlying subscription credential that the registration service considers current, each renders obvious and alternately provides a "***target credential***" in a manner consistent with the '510 Patent's description of such features. *Supra*, [1d]. Likewise, Salmela's current subscription credential 26 on device 10 that would be

[0003], [0010]-[0012]; EX1003, ¶119. For example, Salmela discloses that subscription credentials 26 "generally remain valid for as long as the owner of the device 10 maintains a corresponding subscription agreement with the home network operator that issued the subscription credentials 26." EX1004, [0022]. Thus, when the user requests to change home operators by canceling a subscription plan, the user is requesting to invalidate the device's current subscription credentials and replace them with a target credential associated with a new home operator. EX1004, [0007]-[0009], [0022]; EX1003, ¶120.

To the extent Salmela does not expressly disclose that device 10 obtains an indication of a user request to update a subscription plan ***through a user interface*** of device 10, this conventional option would have been obvious to a POSITA based on the teachings of Rishy-Maharaj. EX1003, ¶121. As described above in connection with [1a], Rishy-Maharaj discloses a wireless device 102 including a user interface. EX1005, [0028]-[0046], [0058]-[0060], [0066], [0067], [0108]-[0121], FIGS. 1A, 1B, 2. Rishy-Maharaj further discloses that a "user may select

---

replaced when the subscription is changed can be indicated by a hash value, time stamp, or the underlying credential 26 itself, each of which maps to and renders obvious a "***particular credential***" as claimed. EX1004, [0041], [0044]; EX1003, ¶119.

[a] subscription plan … that best suits the user", and in particular, "[t]he wireless device 102 may [] have an optional user input 120 to allow the user to select a plan." EX1005, [0112]; *see also*, [0108]-[0121], FIGS. 1B, 2.

As described above in §V.A.3, it would have been obvious for a POSITA to implement Salmela in accordance with Rishy-Maharaj's teaching such that the user in Salmela would submit a request to change subscription plans through a user interface of his or her device 10. EX1003, ¶122. Doing so would, among other reasons discussed above, enhance the user's convenience in selecting or changing a subscription plan. EX1003, ¶122; *supra*, §V.A.3. As a result, Salmela's device 10 in the combination would obtain, through the user interface and based on the user's selection of a new subscription plan in the user interface, an indication of a user request to replace a particular credential (e.g., subscription credential 26) with the target credential (e.g., a new credential associated with the new subscription plan) as recited in Element [1f]. EX1003, ¶122; *cf.* EX1001, 12:45-14:40 and FIGS. 4-13 ('510 Patent similarly describing embodiments where the device obtains an "indication" of a user request to replace credentials based on the user's mere tapping of a "Transfer" button).

Element [1g]

Salmela discloses that device 10 is configured to detect a failure to gain network access using its current subscription credentials 26, and based on such

detection, automatically revert from current subscription credentials 26 to temporary access credentials 30 as part of an automated process for obtaining new subscription credentials associated with a new subscription plan. EX1004, [0010] ("reverts from subscription credentials to temporary access credentials, in response to detecting an access failure"), [0024], [0025] ("device 10 thus (automatically and autonomously) switches from its provisioned subscription credentials 26 to its temporary access credentials 30…to gain temporary network access), [0027], [0033]-[0035] ("detecting a failure to gain network access"), FIG. 4. This failure to gain network access indicates that the device 10 is no longer provisioned with valid credentials due to a possible subscription change and represents ***a network-provisioning state change***. EX1003, ¶123-126; *cf.*, EX1001, 9:4:11, 11:20-27 ('510 Patent describing how denied network access events of the same kind disclosed in Salmela indicate network provisioning state changes).

For example, Salmela discloses that device 10 can "detect access loss for its local (preferred) RAN" using subscription credentials 26. EX1004, [0033]. Based on detecting this access loss, device 10 "attempt[s] reconnection using its current subscription credentials 26." EX1004, [0033]. If reconnection attempts fail, device 10 can "scan for alternative access" and ultimately determine that there has been a failure to gain network access if device 10 is unable to secure alternative access using subscription credentials 26. EX1004, [0034], [0035]. Through these

operations, the device 10 detects a "***network-provisioning state change***" indicating that current subscription credentials 26 are no longer usable by the device 10 to gain access to services on the network. EX1003, ¶125.

Salmela's device 10 also performs actions to automatically check the validity of its current subscription credentials and obtain new subscription credentials based on detecting a failure to gain network access, as illustrated below in FIG. 2, for example. EX1004, [0027]; *see also* [0033]-[0035], [0037]-[0038], FIG. 4; *infra*, Elements [1h]-[1k]; EX1003, ¶126.

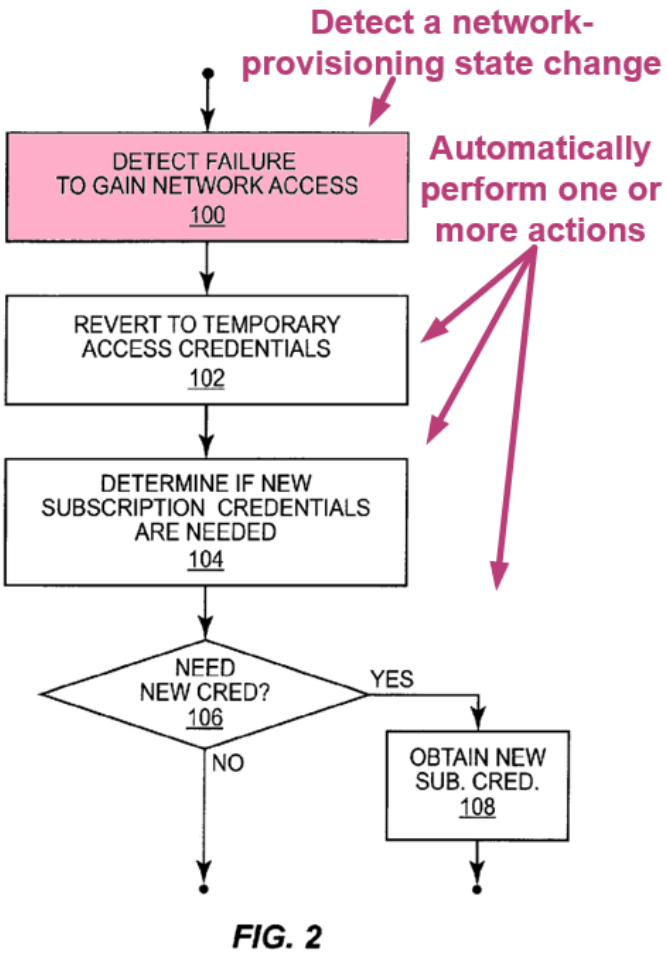


FIG. 2

EX1004, FIG. 2 (annotated).

Element [1h]

Based on detecting a failure to gain network access using its current subscription credentials 26, device 10 automatically reverts to temporary access credentials 30. EX1004, [0010], [0024] ("revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure"), [0027] ("in response to detecting such failure, [] reverting from the current subscription credentials 26 to the temporary access credentials 30"), FIG. 2. Using temporary access credentials 30, device 10 obtains temporary network access and connects with a registration server to determine whether new subscription credentials are available for device 10. EX1004, [0010], [0027] ("determining whether new subscription credentials are needed based on gaining temporary network access via the temporary access credentials"), FIG. 2; EX1003, ¶127-129.

As described above in connection with [1d] and [1f], Salmela's device 10 automatically identifies a need for new subscription credentials by determining that its current subscription credential 26 (***particular credential***) does not match the subscription credential that the registration service considers to be current (***target credential***). EX1004, [0041], [0044]; *supra*, [1d], [1f]. Salmela describes options for determining this mismatch by comparing either hash values or time stamps respectively associated with the device's current subscription credential 26 and the

credential that the registration service considers current, although it would have been equally obvious to directly compare the underlying credentials themselves.[4] EX1004, [0041], [0044], *see also* [0020]-[0027]; *supra*, Elements [1d], [1f]; EX1003, ¶130-132.

A process for automatically determining that new credentials based on detecting a ***network-provisioning state change*** is depicted below in FIG. 2 of Salmela:

[4] Recall that Salmela's hash values, time stamps, and underlying credentials (e.g. IMSI) all provide alternative forms of the claimed "***particular credential***" and "***target credential***" consistent with disclosures in the '510 Patent itself. *Supra*, [1d], [1f]; EX1003, ¶130.

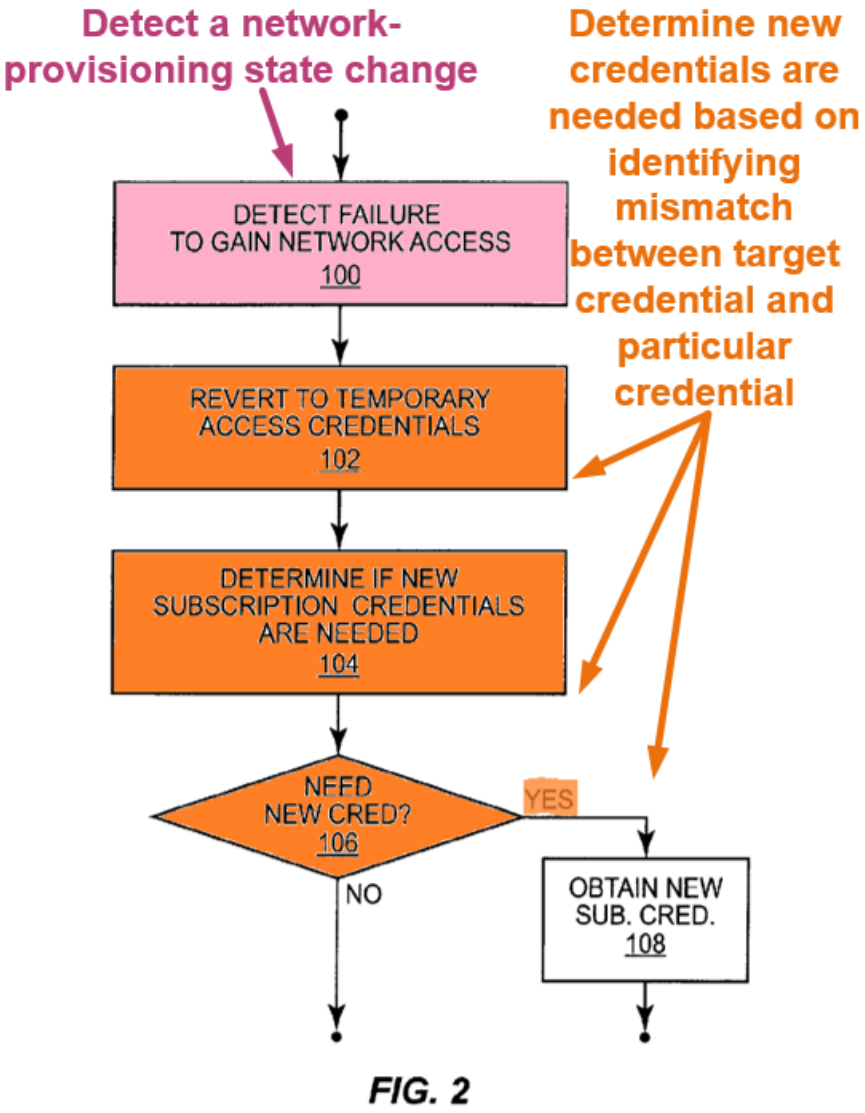
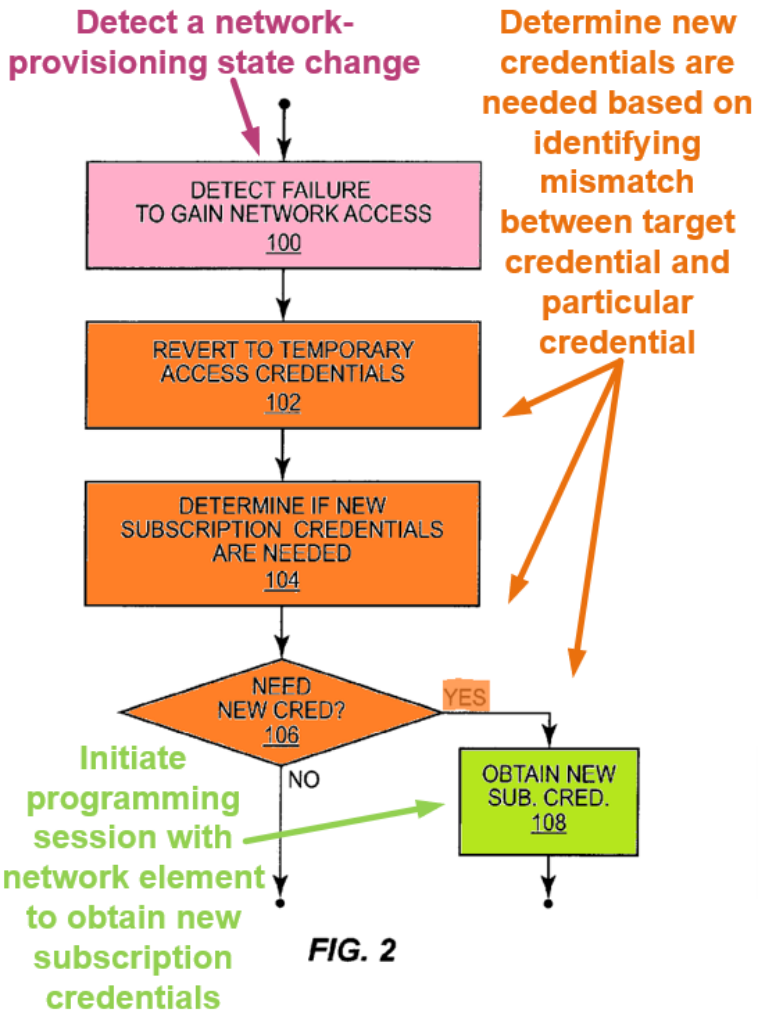


FIG. 2

EX1004, FIG. 2 (annotated).

Element [1i]

Salmela discloses that device 10 can ***initiate*** a ***programming session*** with a ***network element*** to obtain new subscription credentials. EX1004, [0025]-[0027]; EX1003, ¶133-137. An example process for automatically initiating a programming session to obtain new subscription credentials is depicted below in FIG. 2:



EX1004, FIG. 2 (annotated).

To obtain the new subscription credentials, Salmela's device 10 receives "network address information from the registration service that identifies a credentialing server from which the new subscription credentials are to be obtained." EX1004, [0045]; EX1003, ¶134. Using this network address information, device 10 initiates a programming session with a "credentialing server"—a ***network element***—to obtain the new subscription credentials. EX1004, [0045] ("using the temporary network access to contact the credentialing server to

obtain the new subscription credentials"), [0025]. Device 10 ***automatically*** performs these operations based on its detection of a network access failure (***network-provisioning state change***). EX1004, [0011] ("devices [] ***autonomously*** detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials"), [0048] ("***automatic*** acquisition of new subscription credentials"), [0025], claim 25; EX1003, ¶135.

Salmela's ***network element***—e.g., the "credentialing server"— is communicatively coupled to device 10 over the wireless access network. EX1003, ¶136. For example, Salmela discloses that "the credentialing server is, in one or more embodiments, an entity in…the CN of the service provider that issued the new subscription credentials." EX1004, [0045]. In the telecommunications field, "CN" refers to "core network," which is an aspect of a wireless access network and which can be accessed through the radio access network ("RAN") of the wireless access network. EX1004, [0028], FIG. 3; EX1003, ¶136 (citing corroborating EX1017, 6, EX1018, 2).

The credentialing server is located in the core network of the wireless access network that issues subscription credentials for the device 10 to access one or more services. EX1004, [0028], FIG. 3. Device 10 is accordingly communicatively

coupled to the credentialing server over the wireless access network. EX1003, ¶137.

Element [1j]

Through the ***programming session*** initiated with the ***network element*** ("credentialing server"), device 10 can obtain an ***updated credential*** (e.g., a new subscription credential 26) from the credentialing server.[5] EX1004, [0025], [0027], [0045] ("using the temporary network access to contact the credentialing server to obtain the new subscription credentials"), FIGS. 2, 4. The updated subscription credential obtained from the credentialing server and associated with the new subscription plan replaces the subscription credentials 26 on device 10 associated with the prior subscription plan.[6] EX1003, ¶138. Device 10 obtains the updated

[5] Like Salmela, the '510 Patent explains that the updated credential can be the target credential or the target credential can be a representation of the updated credential. EX1001, 9:16-19 ("mobile device 100 detects that a current device credential does not match the expected credential"), 9:47-49 ("delivers the new device credentials to the device"), 10:42-44 ("stores the expected credentials to be programmed to mobile device 100"); EX1003, ¶138.

[6] In at least two instances, Salmela uses both of the terms "new" and "updated" to refer to subscription credentials obtained using temporary access credentials.

subscription credentials ***automatically*** through the process that occurs based on the device's detection of a network access failure (***network-provisioning state change***). EX1004, [0011] ("devices [] ***autonomously*** detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials"), [0048] ("***automatic*** acquisition of new subscription credentials"), [0025], claim 25; EX1003, ¶138.

Element [1k]

Salmela teaches, for example, that device 10 "uses its temporary access to obtain new subscription credentials, which it may download to its secure element 24." EX1004, [0025], *see also* [0036] ("Once the device 10 obtains new subscription credentials, they replace its previously current subscription credentials, and the newly obtained subscription credentials become the device's current subscription credentials 26."), [0046] ("replace or deactivate its formerly current subscription credentials ..."). As described above in connection with

---

EX1004, [0011] ("new/updated subscription credentials"), [0036] ("[t]he device 10 then uses that temporary network access to obtain new subscription credentials (Block 126), which comprises downloading a new or updated USIM"). Salmela further teaches that "[o]nce the device 10 obtains new subscription credentials, they replace its previously current subscription credentials." EX1004, [0036].

Element [1b], *supra*, the memory of device 10 includes secure element 24. EX1004, [0020], [0025]. Device 10's processors thus assist in storing the updated credential (e.g., the "new subscription credential") in the memory. EX1003, ¶139. The updated credentials replace the prior subscription credentials ***automatically*** based on the device's detection of a network access failure (***network-provisioning state change***). EX1004, [0011] ("devices [] ***autonomously*** detect problems with their current subscription credentials, and use their temporary access credentials to gain new/updated subscription credentials"), [0048] ("***automatic*** acquisition of new subscription credentials"), [0025], claim 25; EX1003, ¶139.

Claim [2]

Salmela discloses that its process of checking for and updating subscription credentials is a recurring process that occurs whenever current subscription credentials are unable to provide network access. EX1004, [0010], [0020]-[0027], FIGS. 1-2; *supra*, Elements [1g]-[1k]; EX1003, ¶140-144. This process can result in current subscription credentials 26 being replaced with new/updated subscription credentials. EX1004, [0025], [0027]. The new/updated subscription credentials then become the current subscription credentials, replacing the previous credentials that failed to gain network access. EX1004, [0036], [0046]; *supra*, Element [1k]. After device 10 replaces a ***particular credential*** (e.g., current subscription credentials 26) with an ***updated credential*** (e.g., new subscription

credentials) as described in Elements [1f]-[1k], *supra*, device 10 uses the same automatic process to replace the ***updated credential*** (e.g., new subscription credentials) when Salmela's device 10 detects that the new subscription credentials fail to gain network access. EX1004, [0046] ("in case further reversions are needed"); EX1003, ¶140.

After the ***updated credential*** (e.g., new subscription credentials) replaces the ***particular credential*** (e.g., the previously current credential) based on device 10 detecting a network access failure using the ***updated credential***, device 10 can perform another comparison—this time between a hash value corresponding to the ***target credential*** (which the registration service considers to be current for device 10) and a hash value corresponding to the ***updated credential*** (which is now the current subscription credential 26). EX1004, [0020]-[0027], [0041], [0044] [0049]-[0056], FIGS. 1-2; *supra*, Elements [1g]-[1k]; EX1003, ¶141-142. A POSITA would have understood and it would have been obvious that a mismatch would be determined between the hashes for the ***updated credential*** and ***target credential*** if the value of the ***target credential*** changes for any reason after the device begins using its ***updated credential*** as the current subscription credential. EX1003, ¶142. The mismatch can also be determined based on comparison of time stamps or the underlying credentials, as described above. *Supra*, [1d], [1k].

Salmela teaches that the value of the ***target credential*** can change, for example, when the user makes another request to change the home operator or subscription plan thereby causing the registration service to update the ***target credential*** according to the request.[7] EX1004, [0010]-[0012], [0050], FIGS. 2, 4. Even if the user has not requested to activate a new subscription plan or to change the home operator and the ***target credential*** has not changed at the registration service, it would have been obvious that the device 10 would still detect a mismatch between the hashes for the ***updated credential*** and ***target credential*** if the hashes or the credentials themselves have been corrupted at device 10 (e.g., as a result of transmission or memory errors). EX1003, ¶143 (citing corroborating EX1019, 4).

Based on determining that the updated credential does not match the target credential, device 10 can take an ***action***, e.g., "identify[ing] a credentialing server from which [] new subscription credentials are to be obtained, and using the

[7] The '510 Patent confirms that the target credential—sometimes referred to as the "requested credential" or "expected credential"—is not necessarily static. The value of the target credential can change whenever a new phone number or other credential is submitted as the target of a phone number or other credential porting process. EX1001, 9:11-27, 10:42-51, 7:1-15, FIG. 2; EX1003, ¶143.

temporary network access to obtain the new subscription credentials." EX1004, [0045]; *see also*, [0026], [0027]; *infra*, Claims [3], [6]; EX1003, ¶144.

Claim [3]

Salmela explains that the ***updated credential*** obtained to replace the ***particular credential*** becomes the current subscription credential 26 that device 10 uses "unless and until it is unable to gain access using those credentials." EX1004, [0024], *see also* [0025], [0027], [0045]. Based on detecting that the ***updated credential*** fails to provide network access, device 10 can determine that the ***updated credential*** does not match the ***target credential***. EX1004, [0024], [0027], [0033]-[0035], [0041]. Device 10 can communicate with the ***network element*** (e.g., credentialing server) to replace the ***updated credential*** based on this determination, just as device 10 previously communicated with the credentialing server to replace the ***particular credential***. EX1004, [0045]; EX1003, ¶145.

Claim [6]

Salmela discloses that device 10 reverts from the current subscription credentials 26 to temporary access credentials 30 based on determining that the current subscription credentials fail to provide network access. EX1004, [0010], [0024], [0027], FIG. 2; *supra*, Claim [2]. These temporary access credentials 30 provide "temporary, limited network access" which is a lesser, restricted form of access to the network as compared with the access provided by valid subscription

credentials 26. EX1004, [0006], [0007], [0012], [0020], [0022]-[0024]; EX1003, ¶146. For example, temporary access credentials 30 allow the device to communicate with a registration server but may restrict access to other services that would be available by valid subscription credentials 26. EX1004, [0020]-[0027]. Consequently, by reverting to the temporary access credentials 30, device 10 ***at least assists*** in ***restricting communications*** by device 10 over the ***wireless access network***. When device 10 detects that the ***updated credential*** does not match the ***target credential***, device 10 continues using the temporary access credentials 30 that offer limited network access. EX1004, [0045] ("using the temporary network access to contact the credentialing server"); EX1003, ¶146-147.

Claim [7]

Salmela's ***updated credential*** (e.g., new subscription credentials) can replace the formerly current subscription credentials 26 representing the ***particular credential*** to become the current subscription credentials stored in secure element 24. EX1004, [0020]-[0027], [0036], [0040], [0041], [0044]-[0047]; *supra*, Elements [1g]-[1k]; EX1003, ¶148-151. When device 10 replaces current subscription credentials 26 with new subscription credentials, device 10 retains temporary access credentials 30 "in case further reversions are needed." EX1004, [0046]. Indeed, Salmela discloses that another reversion to temporary access credentials 30 is needed when the ***updated credential*** represented by the new

subscription credentials fails to gain network access. EX1004, [0047]. Salmela's device 10 can determine whether a new subscription credential is needed based on comparing a hash value or other information about the ***updated credential*** (e.g., the new current subscription credential 26) with a hash value or other information about the ***target credential*** (e.g., subscription credentials considered by the registration service to be "current" for device 10). EX1004, [0041], [0044].

When device 10 determines that the ***updated credential*** matches the ***target credential*** based on comparing the hash values, device 10 ***takes an action*** to return to using the ***updated credential***. EX1004, [0047] ("returns to using its current subscription credentials 26"). In this context, a POSITA would have understood and it would have been obvious that a match would be determined between the ***updated credential*** and the ***target credential***, for example, when the user has not requested to activate a new subscription or to change home operators and the target credential held by the registration service has not changed since the device 10 began using the ***updated credential***. EX1004, [0040]-[0044], [0053]; EX1003, ¶151.

Claim [11]

Detecting a failure to provide network access involves, in certain cases, ***determining*** that a ***registration attempt*** initiated by Salmela's device 10 has ***failed***. EX1004, [0027], [0024], [0033]-[0035], [0037], [0038]; EX1003, ¶152-153. For

example, Salmela discloses that "[i]n … detecting network access failure, the device 10 experiences a loss of its home network …which may mean that the device 10 can communicate with a local RAN, but is not recognized or otherwise authenticated by its home network." EX1004, [0037]. The lack of recognition of device 10 or other failure to authenticate with a home network would result from a failed registration attempt. EX1003, ¶152.

In further examples, Salmela explains that the device 10 can detect failed network access resulting from access loss for its local RAN or from being "explicitly disconnected from its home network." EX1004, [0033], [0038]. Such a disconnection from the home network would result from a failure of the device 10 to register with the home network. EX1003, ¶153. For example, when device 10 is not properly registered with the home network in Salmela's "registration service," subscription credentials 26 would not be "considered by the registration service to be current" for device 10 to access the home network that device 10 failed to register with. EX1004, [0044].

Claim [14]

Salmela acknowledges that provisioning a wireless device with subscription credentials allows the device to authenticate itself to a home operator for a given subscription. EX1004, [0003]; EX1003, ¶154-155. Consequently, when device 10 detects that the current subscription credentials 26 of device 10 fail to provide

access to a home operator network, device 10 likewise determines that an ***attempt*** by device 10 to ***authenticate*** with the ***network element*** has ***failed***. EX1003, ¶154. Furthermore, Salmela discloses that one example of detecting network access failure involves device 10 not being recognized "or otherwise ***authenticated***" by its home network which includes the ***network element*** (e.g., the credentialing server). EX1004, [0037]; EX1003, ¶155.

Claim [15]

Salmela discloses that device 10 can "detect access loss for its local (preferred) RAN" using the current subscription credentials 26. EX1004, [0033]. In response to detecting this access loss for the local RAN, device 210 can "attempt reconnection using its current subscription credentials 26—e.g., using its stored IMSI for some number of attempts." EX1004, [0033]. If these reconnection attempts are unsuccessful, device 10 "scans for alternative access" to non-preferred networks. EX1004, [0034]. If this fails, device 10 determines that subscription credentials 26 fail to provide network access, thus detecting a network-provisioning state change. EX1004, [0035]. Salmela also discloses that a failure to gain network access can result from the device 10 not being "recognized or otherwise authenticated by its home network." EX1004, [0035]; EX1003, ¶156.

These attempts to reconnect with the preferred network and connect with non-preferred networks represent failed attempts by device 10 to be authorized for

the service(s) provided by these networks, such as voice services, data services, and/or Internet services. EX1004, [0003] ("network ***service*** provider (home operator)"), [0004] ("access subscribed services"), [0028] ("Internet"), [0033]-[0035], FIG. 3; EX1003, ¶157. When device 10 is unable to connect to the preferred and non-preferred networks using its current subscription credentials 26, a POSITA would have understood and it would have been obvious that device 10 has determined that an ***attempt*** by the device 10 to be ***authorized*** for ***services*** on these networks has ***failed***. EX1003, ¶157.

Claim [16]

Salmela teaches that device 10 can detect a failure of subscription credentials 26 to provide network access by determining that a network access error has occurred. EX1003, ¶158. For example, the network access error may be determined by detecting a number of unsuccessful attempts in using subscription credentials 26 to gain network access. EX1004, [0024] ("device 10 uses its subscription credentials 26 for gaining network access unless and until it is unable to gain access using those credentials"), [0027] ("the method includes detecting a failure to gain network access using the current subscription credentials 26 held in the wireless communication device 10"), [0037] ("not recognized or otherwise authenticated"), [0038] ("explicitly disconnected … device's subscription credentials are expired or otherwise invalid").

Claim [17]

Salmela's device 10 can identify the failure of subscription credentials 26 to provide network access by receiving a provisioning-state change message (e.g., "failure message") which indicates the network access failure. EX1004, Claim 14 ("the wireless communication device is configured to detect a failure to gain network access…based on receiving a failure message responsive to attempting to gain network access using the current subscription credentials"), [0038] ("home network sends signaling—e.g., a message—to the device 10 that indicates that the device's subscription credentials are expired or otherwise invalid" and "device 10 recognizes such signaling as an explicitly indicated network access failure"). Receiving this failure message represents detecting a network provisioning-state change and indicates that the device 10 is no longer provisioned for network access using the subscription credentials. EX1003, ¶159.

Claim [18]

As a first matter, it would have been obvious for Salmela's "failure message" to include ***text*** and therefore comprise a ***text message***, because there are a limited number of ways to communicate a failure in a message and a ***text message*** is a prominent solution to achieve this. EX1003, ¶160-162. Implementing the failure message to include a text message would have been particularly

obvious, for example, to provide a notification that would permit the failure message to be presented to and read by the user. EX1003, ¶160.

Even if Salmela itself does not expressly disclose or render obvious implementing the failure message as a text message, Rishy-Maharaj describes various conventional communication channels that can be utilized for signaling between a wireless device and network elements including "short message service" ("SMS") protocols. EX1005, [0036], [0109], [0182]; *see also* [0028]-[0035], [0108]-[0121]. SMS is widely known in the field to refer to protocols for text messaging. EX1003, ¶161. It would have been obvious to communicate Salmela's network access failure message as a text message using the SMS protocol as suggested by Rishy-Maharaj to allow the failure message to be read by a user and to avoid roaming charges that could otherwise be incurred before a home operator switch is complete. EX1005, [0036]; EX1004, [0009], Claim 14. The use of SMS-based text messages also would have been obvious to try in light of the limited number of communication channels available to the wireless device, and further would have been obvious as a straightforward application of a known technique (e.g., SMS-based messaging) to a known system (e.g., Salmela's) to achieve merely predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶160-162.

Claim [19]

Salmela discloses that the "home network [can] send[] signaling—e.g., a message—to the device 10 indicating that the device's subscription credentials are expired or otherwise invalid" and "device 10 recognizes such signaling as an explicitly indicated network access failure." EX1004, [0038]; *see also*, Claim 14. The "failure message" described in paragraph [0038] and claim 14 of Salmela is not requested by the device but is instead pushed from the home network server (***push server***) communicatively coupled to the ***wireless device*** over the ***wireless access network*** of the home operator. EX1004, [0028], FIG. 3; EX1003, ¶163-164. Multiple references corroborate that it was well known for wireless devices to receive push messages from push servers by 2013. EX1003, ¶165 (citing corroborating EX1015, 96; EX1016, 140; EX1020, 101; EX1021, 81).

That the failure message is pushed to the wireless device would have been evident, or at least obvious, to a POSITA since the failure message is automatically sent from the home network to the wireless device as an explicit indication of network access failure, as opposed to other instances where device 10 detects a network provisioning state change as a result of the device's inability to communicate with the local RAN or inability to be authenticated over the local RAN. EX1004, [0033], [0037], FIG. 4; EX1003, ¶166. The use of push messages also would have been obvious to try in view of the limited number of communication channels available to the wireless device, and further would have

been obvious as a straightforward application of a conventional technique (e.g., push notifications) to a known system (e.g., Salmela's) to achieve merely predictable results. *KSR*, 550 U.S. at 417; EX1003, ¶166.

Claim [20]

Salmela discloses that the device 10 includes logic that enables it to "recognize[]" a network-provisioning state change message (e.g., a network-access failure message) "as an explicitly indicated network access failure." EX1004, [0038]. Salmela also explains that processing on the device 10 is "implemented via software executing in one or more microprocessor circuits." EX1004, [0026]; *see also* [0020] ("storing working data, computer program instructions"). A POSITA would have appreciated and found obvious that Salmela's software for receiving and processing the network-access failure message constitutes an ***application program*** on the wireless device (e.g., device 10), especially since application programs commonly refer to software like that disclosed in Salmela. EX1003, ¶167-168. Indeed, the '510 Patent broadly describes "application" programs with reference to a range of different types of software including user applications (e.g., "browser"), operating system (OS) applications, and native applications. EX1001, 10:62-64. EX1003, ¶168. Rishy-Maharaj similarly confirms that implementing software like Salmela's as application programs was a known and conventional option before the Critical Date. *See, e.g.*, EX1005, [0062] (describing

"***applications*** necessary to provide instructions to the network and control routines 115").

Claim [21]

Salmela expressly discloses that "the subscription credentials 26 comprise a downloadable Universal Subscriber Identity Module (USIM), which may include an international mobile subscriber identifier (IMSI)." EX1004, [0023], [0033] ("using its stored IMSI"), [0036] ("IMSI-based attachment"), FIG. 4; EX1003, ¶169. A POSITA would have recognized and found obvious that an IMSI is a ***phone number*** consistent with the plain meaning of this term as used in the '510 Patent in that it is a number that uniquely identifies device 10 (e.g., "a cellular radiotelephone") and its USIM.[8] EX1004, [0021], [0023]; EX1003, ¶169.

[8] The '510 Patent does not define the term "phone number," nor does it use the term "phone number" to refer to a specific type of credential or identifier known in the field. EX1003, ¶168. For example, the specification of the '510 Patent provides a lengthy list of credentials that a mobile device may use to authenticate with a wireless network including a phone number, an IMSI, an MSID, an MSISDN, an MDN, and many more. EX1001, 5:21-43. The listed credentials are not mutually exclusive, however. For instance, the MSISDN and MDN are both numbers that a calling party may call to reach a device on cellular network, which are often

Claim [22]

Salmela expressly discloses that "the subscription credentials 26 comprise a downloadable Universal Subscriber Identity Module (USIM), which may include an ***international mobile subscriber identifier (IMSI)***." EX1004, [0023], [0033] ("using its stored IMSI"), [0036] ("IMSI-based attachment"), FIG. 4; EX1003, ¶170-171.

Claim [23]

In cases where the subscription credentials 26 comprise an IMSI ***phone number*** (Claim [21], *supra*) a POSITA would have understood and it would have been obvious that the ***target credential*** would also include an IMSI ***phone number*** so that device 10 would be capable of comparing credentials to determine a match and to update the IMSI when a new subscription is available. EX1004, [0021], [0023], [0041], [0044]; EX1003, ¶172.

---

colloquially referred to as "phone numbers," even though the '510 Patent identifies them alongside "phone number" in the list of credentials. EX1001, 5:21-43. In this context, a POSITA would have understood that the term "phone number" in the '510 Patent does not refer to a specific or particular type of number but instead broadly encompass a range of different numbers that identify or are associated with a wireless device including an IMSI. EX1003, ¶169.

Claim [24]

Salmela discloses that device 10 automatically initiates a process to update a ***particular credential*** (e.g., current subscription credentials 26) of the ***one or more credentials*** with new subscription credentials in response to detecting that the current subscription credentials 26 no longer provide network access. EX1004, [0022]-[0027], [0033]-[0038]. This automatic update is done based on comparing the ***particular credential*** with a ***target credential***. In examples where the current subscription credential 26 includes an "***international mobile subscriber identifier (IMSI)***," a POSITA would have understood and it would have been obvious that the ***target credential*** would also include an ***IMSI*** so that device 10 would be capable of comparing them to determine a match and to update the IMSI when a new subscription is available. EX1004, [0023], [0041], [0044]; EX1003, ¶173-174.

Claim [25]

Because Salmela's ***particular credential*** and ***target credential*** can each comprise an IMSI amounting to a ***phone number*** as described above in connection with claims [21] and [23], *supra*, Salmela's current subscription credentials 26 would represent or at least render obvious a ***first*** IMSI ***phone number*** that is different from a ***second*** IMSI ***phone number*** considered by the registration service "to be current" for device 10 when the credentials have been updated in response

to a requested change in subscription plans or home operator. EX1004, [0010]-[0012], [0023], [0041], [0044]; EX1003, ¶175.

Claim [28]

Salmela discloses types of wireless devices 10 that commonly included displays such as "a cellular radiotelephone, pager, [or] PDA … ." EX1005, [0021]. In the combination, Rishy-Maharaj also expressly discloses that the user interface can include a ***display***. EX1005, [0059] ("[t]he device output system 110 may include… a display system…"), [0067] ("optional display 122 may be any display capable of rendering images, including, by way of example, a monitor, laptop screen, net book screen, cellular phone, smart device, personal desktop assistant or projector"); *supra*, §V.A.3; EX1003, ¶176-177. FIG. 1B of Rishy-Maharaj, which depicts the device output system 110 and optional display 122, is reproduced below:

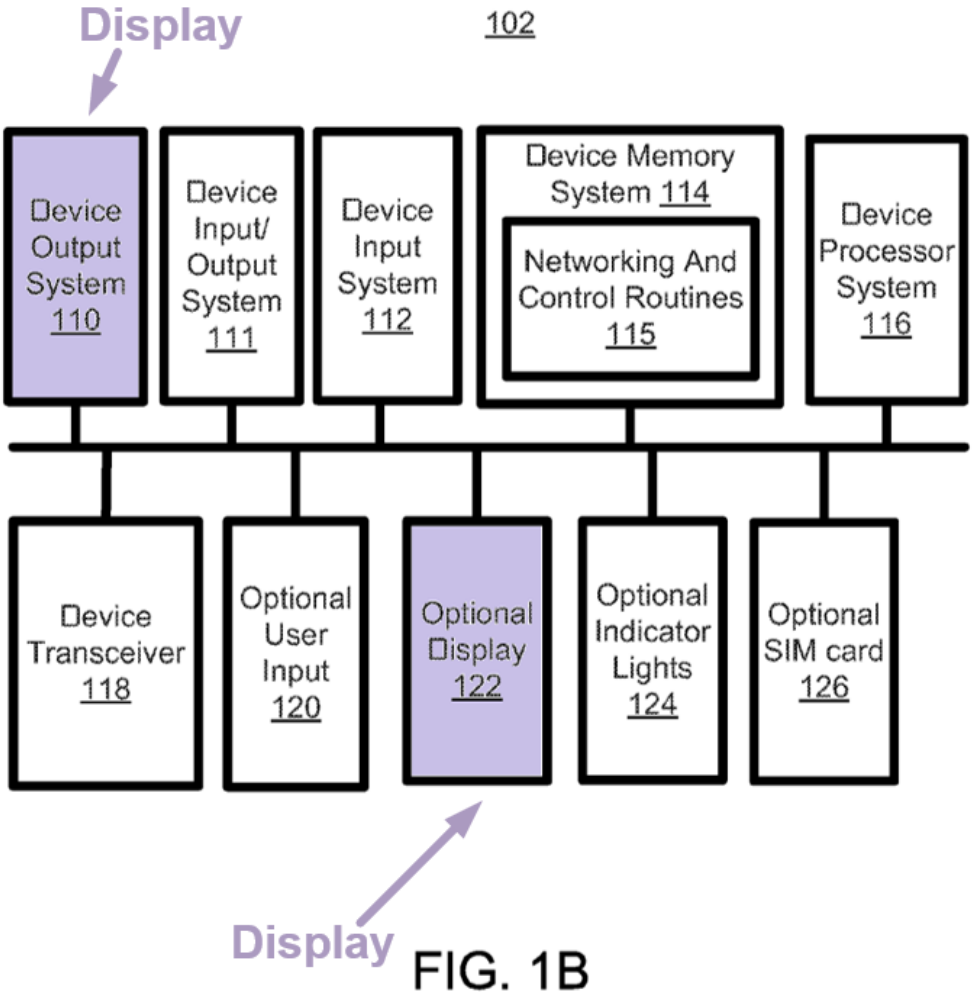


FIG. 1B

EX1005, FIG. 1B (annotated).

Claim [29]

Salmela discloses wireless devices 10 that commonly include ***speakers*** such as "a cellular radiotelephone, pager, [or] PDA … ." EX1005, [0021]. Additionally, in the combination, Rishy-Maharaj expressly discloses that the ***user interface*** can include a ***speaker***. EX1005, [0059] ("[t]he device output system 110 may include… a speaker system…"), [0160], FIG. 1B; *supra*, §V.A.3; EX1003, ¶178.

FIG. 1B of Rishy-Maharaj, which depicts the device output system 110, is reproduced below:

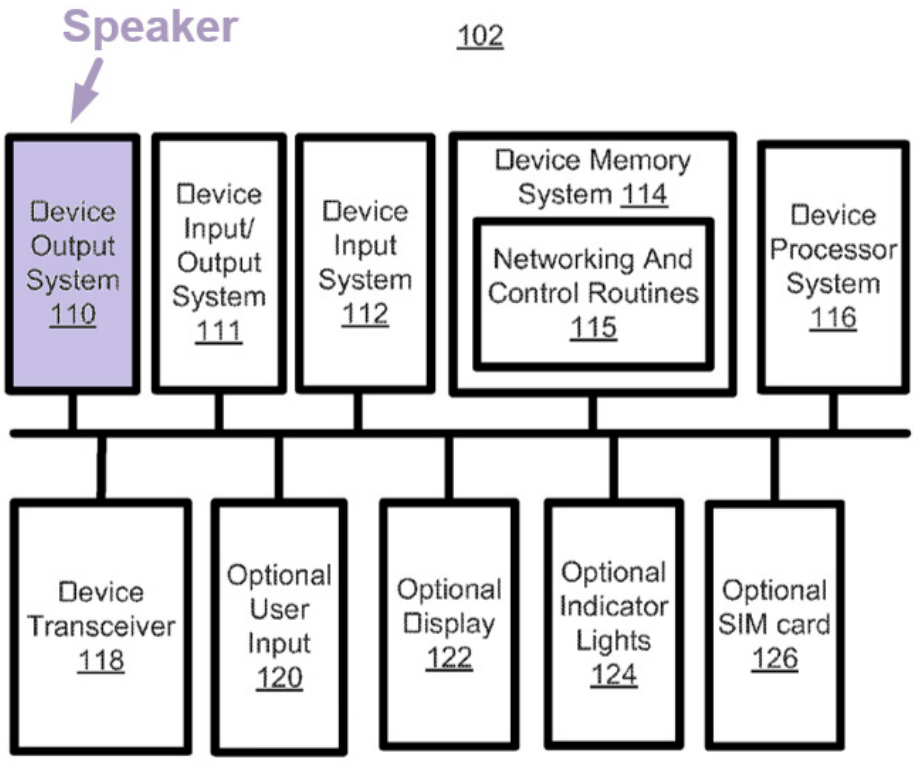


FIG. 1B

EX1005, FIG. 1B (annotated).

Claim [30]

Salmela discloses that device 10 can use its credentials to access home network 40 and visited network 46, which are ***wireless access networks*** including RANs and CNs that provide services to connected devices. EX1004, [0028], [0030]-[0032], FIG. 3. The wireless access networks "communicative[ly] couple to one or more additional networks 52, such as the Internet" thereby providing the

device 10 with access to Internet ***data services***. EX1004, [0028]. A POSITA also would have understood and it would have been obvious that wireless access networks like those described in Salmela commonly provided voice, data, and/or messaging ***services*** that would ordinarily be utilized by a wireless device such as Salmela's "cellular radiotelephone, page, [or] PDA." EX1004, [0021]; *supra*, Claim [18] (describing SMS messaging service); EX1003, ¶179.

For example, Salmela discloses that in some embodiments, "the device 10 is a cellular communication device." EX1004, [0021]. One class of cellular communication devices that use credentials to access networks is "conventional 3G cellular telephones." EX1004, [0004]. 3G cellular telephones receive any one or combination of data service, voice service, and messaging service from wireless access networks such as home network 40 and visited network 46 that include RANs and CNs. EX1003, ¶180. ***Data service***, ***voice service***, and ***messaging service*** are staple services provided by wireless access networks including RANs and CNs, especially networks that operate in accordance with 3G and other 3GPP protocols. EX1005, [0035] ("wireless device 102 may communicate with other networks and devices using any wireless protocol including, for example, Wi-Fi, Wi-Max, 2G, 3G, 4G, 4G LTE, UMTS, other satellite communication, or radio via a transceiver"), [0065]; EX1003 (citing corroborating, EX1018, 2; EX1032, 3).

Claim [31]

Salmela discloses that device 10 includes ***one or more processors*** including processing circuits 20 and credentials processor 22 that execute ***one or more machine-executable instructions***, as described above in connection with Element [1e]. EX1004, [0020], [0024], [0026], [0027], FIG. 1, FIG. 2; *supra*, [1e], [20]. Salmela expressly discloses that the memory (e.g., memory 32) of device 10 can store "computer program instructions," thus indicating that the processing circuits 20 and credentials processor 22 can execute these ***program*** instructions to perform one or more actions. EX1004, [0020]; EX1003, ¶181. It would have been obvious to implement Salmela's machine-executable program instructions as an application program for at least the reasons described above in connection with claim 20. *Supra*, Claim [20]; *cf.* EX1001, 10:62-64 (broad range of example "application" programs in the '510 Patent); EX1003, ¶181. Rishy-Maharaj similarly confirms that implementing software like Salmela's as application programs was a known and conventional option before the Critical Date. EX1005, [0062] (describing "***applications*** necessary to provide instructions to the network and control routines 115"), [0058]; EX1003, ¶181.

Claim [32]

Salmela's ***machine-executable instructions*** include instructions for "obtaining the subscription credentials 26 via over-the-air (OTA) provisioning,"

which renders obvious that Salmela's device 10 includes an ***OTA mobile device parameter programming agent*** to enable device 10 to participate in OTA provisioning. EX1004, [0022]; EX1003, ¶182-184. Salmela also expressly discloses that "credentials processor 22 may be implemented via software executing in one or more microprocessor circuits used to implement the processing circuits 20," which a POSITA would have understood to mean and found obvious that credentials processor 22 can be a ***software agent***. EX1004, [0026]. Furthermore, several references corroborate that it was well known by the 2013 Critical Date of the '510 Patent that a wireless device communicating over a ***wireless access network*** includes an ***operating system***. EX1003, ¶183 (citing corroborating EX1015, 5; EX1016, 1; EX1021, 5).

Rishy-Maharaj likewise discloses a wireless device 102 that includes a device processor system 116 that can "***execute instructions***" in networking control routines 115 stored in a device memory system 114. EX1005, [0063]. Rishy-Maharaj expressly discloses that these networking control routines 115 can "receive credentials to access the then subscribed-to network" and "access the network." EX1005, [0063]. Rishy-Maharaj also discloses that in one embodiment, device processor system 116 is "communicatively coupled to…a wireless modem," e.g., a ***modem programming agent*** or a ***modem software or firmware agent***. EX1005, [0163]; EX1003, ¶184.

Claim [33]

As described above in connection with Element [1f] and the combination overview (§V.A.3), the teachings of Salmela in view of Rishy-Maharaj would have rendered obvious a ***wireless device*** configured to ***receive*** an indication of a ***user request*** to replace a ***particular credential*** with a ***target credential***. EX1004, [0003]-[0009], [0011], [0020]-[0027], [0033]-[0035], [0050]; EX1005, [0028]-[0046], [0058]-[0060], [0066], [0067], [0108]-[0121], FIGS. 1A, 1B, 2; *supra* [1f], §V.A. Salmela and Rishy-Maharaj describe how the ***user request*** can be made by a user selection to activate or change subscription plans. EX1004, [0003]-[0009], [0010]-[0011], [0050]; EX1005, [0066], [0067], [0112], [0113]; EX1003, ¶185-187. For example, Rishy-Maharaj teaches that "[t]he user may use the optional user input 120 to select [a] particular local network subscription that suits the user best." EX1005, [0066], *see also* [0112] ("the user may select the subscription plan and network that best suits the user").

In the combination, Rishy-Maharaj further teaches that the user's request selecting a particular subscription plan includes the user's (subscriber's) ID: "Upon receiving the plan or subscription data, the wireless device 102 or its user may determine that there is a plan … worth purchasing and decide to purchase it. The wireless device 102 may transmit the subscriber ID and the plan selection to the SFSS to process the transaction." EX1005, [0230], FIG. 14 (depicting client device

transmitting request including "SUBSCRIBER_ID, PLAN"); *see also* [0112]-[0113], [0126]-[0127], [0139]-[0140], [0153], FIGS. 4-5. The subscriber ID indicates a ***user name*** or ***subscriber name*** as claimed. EX1003, ¶186. Furthermore, since the user's request identifies a particular plan or network associated with a particular service provider, the user request also includes an indication of a ***company name*** of the service provider that operates the network for the selected plan and an indication of the ***target credential*** associated with the selection. EX1003, ¶187. The request can also include an indication of an ***account number*** that can be charged for the subscription. EX1005, [0153] ("The transaction may include an acceptance of the terms of service of a particular service plan or some agreement to a transaction to add funds or credits to an account."); EX1003, ¶187.

Claim [35]

The Salmela-Rishy-Maharaj combination provides that a wireless device can obtain ***information*** associated with a ***user request*** through a ***user interface*** of the device. EX1005, [0066] ("The user may use the optional user input 120 to select the particular local network subscription that suits the user best."), [0112] ("The wireless device 102 may have an optional display 122 in order to list services and terms of service for the user to select. The wireless device 102 may also have an optional user input 120 to allow the user to select a plan."); EX1003, ¶188.

Claim [36]

Salmela's credentialing server is a network element that performs substantially the same functions as the programming server described in the '510 Patent, including delivering new credentials to the wireless device. *Cf*. EX1001, 9:47-48 ("Programming server 1152 delivers the new device credentials to the mobile device 100."), 7:6-8 ("programming server [] enable[s] the device to obtain the desired credentials") *with* EX1004, [0045] ("credentialing server from which the new subscription credentials are obtained"); EX1003, ¶189. A POSITA also would have understood and found obvious that Salmela's credentialing server comprises a ***programming server*** since the new subscription credentials that device 10 obtains from the credentialing server ***program*** the device 10 to use a wireless access network according to a new subscription plan. EX1004, [0045]; EX1003, ¶189. Indeed, Salmela expressly discloses that device 10 can "download" the new subscription credentials to secure element 24 for use, meaning that device 10 is ***programmed*** with the new subscription credentials. EX1004, [0025]; EX1003, ¶189.

Claim [37]

Salmela explains that device 10 can ***initiate*** a ***programming session*** using temporary access credentials 30, which are part of the ***one or more credentials*** stored in the ***memory*** of device 10. EX1004, [0020]-[0027], FIG. 1; *supra*,

Element [1c]. For example, Salmela discloses that "device 10 is configured to perform a reversion to its temporary access credentials 30, responsive to detecting a network access failure" and "determining whether new subscription credentials are needed…comprises ***contacting a registration service via the temporary network access***." EX1004, [0039], [0040]. The registration service then provides network address information that "identifies a credentialing server from which the new subscription credentials are to be obtained" and the device 10 uses the "temporary network access" obtained with the temporary access credentials 30 "***to contact the credentialing server to obtain the new subscription credentials***." EX1004, [0045]. Consequently, device 10 initiates the programming session with the credentialing server using ***at least a portion*** of the ***one or more credentials*** (e.g., temporary access credentials 30) associated with the ***wireless device***. EX1003, ¶190.

Claim [38]

Salmela expressly discloses that device 10 uses a ***temporary credential*** (e.g., a temporary access credential 30) to contact the ***network element*** (e.g., the credentialing server). EX1004, [0025] ("device 10…uses those temporary access credentials 30 to gain temporary network access"), [0045] ("using the temporary network access to contact the credentialing server to obtain the new subscription credentials"); EX1003, ¶191.

Claim [39]

Salmela discloses that "device 10 includes a 'credentials processor' 22 that is configured to revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure." EX1004, [0024]; *see also* [0010], [0027]-[0028], [0035], [0038], [0047], FIG. 1. The temporary access credentials 30 are stored in the fuse/OTP memory element 28 of device 10. EX1004, [0020], [0023], FIG. 1. Computer processors like Salmela's credential processor 22 are configured to obtain data and instructions from memory to enable the processor to perform operations or other processing on the data according to the retrieved instructions. EX1004, [0020] ("working data, computer program instructions"); EX1003, ¶192-193. A POSITA thus would have understood and it would have been obvious that Salmela's credentials processor 22 obtains the temporary access credentials 30 from fuse/OTP memory element 28 when reverting from the subscription credentials 26 to the temporary access credentials 30. EX1003, ¶193.

Claim [41]

Salmela discloses that device 10 ***initiates*** a ***programming session*** with a ***network element*** (e.g., "credentialing server") using temporary access credentials 30, which represent ***a default credential*** stored in the ***memory*** of device 10. EX1004, [0020]-[0027], FIG. 1; EX1003, ¶194-195. For example, Salmela

discloses that "determining whether new subscription credentials are needed…comprises ***contacting*** a registration service via [] temporary network access." EX1004, [0039], [0040], [0045]. The registration service then provides network address information that "identifies a credentialing server from which the new subscription credentials are to be obtained." EX1004, [0045]. Device 10 uses temporary access credentials 30 and the network address information to "obtain the new subscription credentials." EX1004, [0045].

It would have been obvious that temporary access credentials 30 constitute a ***default credential*** of device 10. EX1003, ¶195. For example, device 10 reverts by default to temporary access credentials 30 anytime that subscription credentials 26 cannot gain network access. EX1004, [0024] ("revert from the subscription credentials 26 to the temporary access credentials 30, responsive to detecting network access failure"), [0025] ("device 10 thus (automatically and autonomously) switches from its provisioned subscription credentials 26 to its temporary access credentials 30, and uses those temporary access credentials 30 to gain temporary network access"). Indeed, temporary access credentials 30 can be "burned into secure fuses or other secure OTP memory within the device 10, during its manufacture or initial configuration" thereby rendering the temporary access credentials 30 available to the device 10 as the ***default credentials*** when temporary network access is needed. EX1004, [0023], [0020]; EX1003, ¶195.

Claim [42]

To ***initiate*** a ***programming session*** with Salmela's network element (e.g., "credentialing server")—which is part of a CN in a ***wireless access network***—it would have been obvious to a POSITA for device 10 to communicate with the credentialing server ***over a wireless access network*** such as the home network of the service provider that issued the new subscription credentials (e.g., home network 40) or another network that serves as a "preliminary" or "registration" operator. EX1004, [0028]-[0029], *see also* [0045]; EX1003, ¶196.

Claim [43]

To the extent Salmela does not expressly disclose that device 10 ***initiates*** the ***programming session*** by communicating with the network element ***over a Wi-Fi network***, this feature would have been obvious based on the teachings of Rishy-Maharaj. EX1003, ¶197-198. For example, Rishy-Maharaj discloses that "wireless device 102 may communicate with other networks and devices using any wireless protocol including, for example, Wi-Fi." EX1005, [0035]. Rishy-Maharaj also discloses that "the wireless device may connect to the SFSS 108 via a routing

network" and "[t]he routing network may be any type of network including…a Wi-Fi network."[9] EX1005, [0109]; *see also* [0036], [0065], [0075], [0089], [0187].

It would have been obvious to implement Salmela's system in accordance with Rishy-Maharaj's suggestion for communicating with a credentialing server over a Wi-Fi network such that device 10 in the Salmela-Rishy-Maharaj combination would communicate over a Wi-Fi network to initiate the programming session with the credentialing server. EX1003, ¶198. A POSITA would have been motivated to configure device 10 to communicate with the credentialing server over a Wi-Fi network to improve device 10's ability to retrieve updated credentials when other types of networks (e.g., cellular networks) are limited or unavailable and to avoid roaming charges that could otherwise be incurred by communicating on certain networks (e.g., visitor networks). EX1005, [0037]-[0038], [0187]; EX1003, ¶198. A POSITA would have reasonably expected success implementing these features in the combination since Wi-Fi networks were ubiquitous by the Critical Date and wireless devices commonly communicated over Wi-Fi networks by this time. EX1003, ¶198. Salmela also does not restrict the

[9] The SFSS 108 of Rishy-Maharaj is a credentialing server that wireless device 102 communicates with to retrieve credentials. EX1005, [0041]-[0042], [0049]-[0050], [0108]-[0118].

types of networks that device 10 may communicate over. *See, e.g.*, EX1004, [0028], [0031], [0057] ("may be implemented in a variety of systems and device types"); EX1003, ¶198.

Claim [45]

As described above in connection with Claim [6], *supra*, Salmela discloses that device 10 reverts from the current subscription credentials 26 to temporary access credentials 30 based on determining that the current subscription credentials 26 fail to provide network access. EX1004, [0010], [0024], [0027], FIG. 2; EX1003, ¶199. Device 10 uses this temporary network access to determine if new subscription credentials are needed and, if so, to obtain the new subscription credentials. EX1004, [0027]. When device 10 obtains the new subscription credentials, these new credentials replace the former subscription credentials and become the current subscription credentials that device 10 uses to gain access. EX1004, [0046].

Temporary access credentials 30 provide "temporary, limited network access" which is a lesser form of access to the network as compared with the access provided by valid subscription credentials 26. EX1004, [0006], [0007] [0012], [0020], [0022]-[0024]; EX1003, ¶199. Consequently, by reverting to the temporary access credentials 30 until new subscription credentials are received, the processors of device 10 ***at least assist*** in ***restricting communications*** by device 10

over the ***wireless access network*** until the ***updated credential*** has been obtained. EX1003, ¶200.

Claim [46]

As described above in connection with Elements [1d] and [1h], Salmela's device 10 determines whether it needs new subscription credentials by comparing information about its current subscription credentials 26 to a ***target credential*** such as "a time stamp or hash value for subscription credentials that are considered by the registration service to be current for the wireless communication device 10." EX1004, [0044], [0041]; *supra*, [1d], [1h]; EX1003, ¶201-203. Salmela's target credential indicates a configuration state of the device 10 by identifying which credentials the network has currently configured for device 10 to be able to access the wireless network associated with the device 10's active subscription plan. EX1003, ¶201. In this regard, Salmela's target credential is substantially similar to the configuration state indicator tersely mentioned in the '510 Patent itself. *Cf.* EX1001, 11:32-37 ("the requested credential may be a configuration state indicator, and the device inspects the configuration state indicator to determine if the device expected additional credential updates associated with the credential change request"). For example, the hash value (or time stamp) that device 10 receives from the registration service can indicate a configuration state by indicating if device 10's current subscription credentials 26 are valid or if device

10 should be reconfigured with new subscription credentials that the registration service considers to be current. EX1004, [0044], [0041]; EX1003, ¶201.

Element [47pre]

See [1pre], [1e]; *see also* EX1004, [0020] ("The device 10 also includes a memory 32, which may include one or more memory devices, for storing working data, computer program instructions, and configuration information."), [0026] ("software executing in one or more microprocessor circuits used to implement the processing circuits 20"), FIG. 1; EX1003, ¶204.

Element [47a]

See [1c], [1d], [1f]; EX1003, ¶205.

Element [47b]

See [1g]; EX1003, ¶206.

Element [47c]

See [1h]; EX1003, ¶207.

Element [47d]

See [1i]; EX1003, ¶208.

Element [47e]

See [1j]; EX1003, ¶209.

Element [47f]

See [1k]; EX1003, ¶210.

Claim [48]

Salmela's current subscription credentials 26 provide a ***particular credential*** that device 10 can replace if the current subscription credentials 26 do not match a ***target credential***. EX1004, [0020]-[0027], [0033]-[0041]; EX1003, ¶211-212 The part of Salmela's ***memory*** that stores current subscription credentials 26 is a ***protected memory***—secure element 24. EX1004, [0020], FIG. 1. Because subscription credentials 26 provide access to networks (e.g., home network 40 and visited network 46) that subscribers ordinarily pay to access and that would create substantial disruption in the ability to connect to a network if the credentials 26 were compromised, it would have been obvious to implement Salmela's secure memory 24 to prevent direct user modification of the subscription credentials 26 stored therein. EX1003, ¶211.

A POSITA would have sought to configure the secure memory 24 in this manner to ensure users could not tamper with the subscription credentials to gain improper access to a subscriber network. EX1003, ¶212. Additionally, preventing direct user modification of information in secure memory 24 is consistent with conventional security features of secure memories by the Critical Date of the '510 Patent. EX1003, ¶212 (citing corroborating EX1028, [0050], EX1029, 3:1-3, EX1030, [0109]).

VI. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. Discretionary denial under §325(d) is not warranted

This Petition does not present a situation where "the same or substantially the same prior art or arguments" were previously considered by the Office to warrant denial under § 325(d). *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,* IPR2019-01469, Paper 6 (Feb. 13, 2020 (Precedential)). Although Salmela was cited in an IDS during prosecution as one of more than *1,500 references* listed on the face of the patent, Salmela was never substantively addressed in any office action or remarks in connection with original examination of the '510 patent. EX1001, Cover; EX1002; *supra*, §II.B. Rishy-Maharaj was never cited at all, and thus never considered in combination with Salmela. For this reason alone, such "new, noncumulative prior art asserted in the Petition" weighs against discretionary denial. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (Oct. 16, 2019 (§§II.B and II.C precedential)). Even if the Examiner had considered any prior art containing teachings cumulative to the teachings of the references cited in this Petition, allowing the '510 Patent over such teachings/prior art amounts to material error in light of the relevance of those teachings to the Challenged Claims as demonstrated herein. These circumstances all counsel against denial under §325(d).

B. Discretionary denial under §314(a) is not warranted

This Petition's merits are compelling, and the evidence presented herein is substantial, counseling against discretionary denial under *Fintiv*. SAMSUNG-1101 4-5. Moreover, the *Fintiv* factors counsel against denial.

Factor 1 is neutral because neither party has requested a stay in the co-pending litigation.

Factor 2 is neutral because the Court's trial date is speculative and subject to change. The Board will likely issue its Final Written Decision around August 2026, approximately six months after the currently scheduled trial date (February 9, 2026). EX1102, 1. However, as the Board/Director have recognized, "scheduled trial dates are unreliable and often change." EX1101, 8.

Factor 3 favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the co-pending litigation in E.D. Tex. is in its early stages. Beyond exchanging preliminary infringement and invalidity contentions, the parties and the court have yet to expend significant resources on invalidity. EX1102. By the anticipated institution deadline in August 2025, the co-pending litigation will still be in early stages—fact and expert discovery will be ongoing, and the Markman hearing will not have occurred. EX1102.

Factor 4 favors institution because Petitioner stipulates to not pursuing the IPR grounds in the co-pending litigation. EX1026. Thus, institution serves "efficiency and integrity goals" by "not duplicating efforts" and "resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5 is neutral. The same parties are in the co-pending litigation.

Factor 6 favors institution because this Petition's merits are compelling, as described herein.

VII. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VIII. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") are the real parties-in-interest. No other party had access or control over this Petition, and no other party provided funding for this Petition.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '510 Patent is the subject of a civil action in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al*, 2-24-cv-00228 (E.D. Tex.), filed April 3, 2024 (EX1100).

Petitioner is concurrently filing a separate IPR petition challenging the '510 Patent in IPR2025-00484.

Petitioner is not aware of any other disclaimers or reexamination certificates addressing the '510 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email:IPR39843-0183IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Nicholas Stephens, Reg. No. 74,320 Cameron A. Ubel, Reg. No. 77,081 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR39843-0183IP1@fr.com (referencing No. 39843-0183IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, monaldo@fr.com, nstephens@fr.com, and ubel@fr.com).

Respectfully submitted,

Dated 02/10/2025

/Nicholas W. Stephens/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Cameron A. Ubel, Reg. No. 77,081
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2025-00483)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,930 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 02/10/2025

/Nicholas W. Stephens/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Cameron A. Ubel, Reg. No. 77,081
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on February 10, 2025, a complete and entire copy of this Petition for *Inter Partes* Review, Notice Ranking Petitions, Power of Attorney and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Diana Bradley/

Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667